Escola Tècnica Superior
d'Enginyeria de Telecomunicació de Barcelona

Diseño y evaluación del traspaso en redes de comunicaciones móviles avanzadas

PROYECTO FINAL DE CARRERA

AUTOR: Daniel Hernández García
DIRECTOR: Antonio Barba Martí

Agradecimientos

Finalmente, después de algún tiempo más de lo previsto inicialmente he llegado al final de mi proyecto final de carrera, y que menos que agradecer el apoyo recibido durante todo este tiempo. Principalmente quiero dar las gracias a mi director de proyecto, Antoni Barba y al doctorante Juan Antonio Guerrero, que reunión tras reunión me aportaban la motivación necesaria en fases difíciles para seguir adelante con la misma ilusión que el primer día. Y como no, gracias a mi familia, que con sus continuas preguntas de ¿cuándo acabas? me ponían la presión necesaria para no tirar la toalla en momentos difíciles. Sin la colaboración de todos no habría conseguido acabar nunca. Muchas gracias.

Resumen

La sociedad actual ha evolucionado ligada a sus avances tecnológicos, cambiando la forma en que las personas se comunican entre ellas y con el mundo. Cada vez más utilizamos servicios proporcionados por las redes de comunicaciones avanzadas para comunicarnos. Mundialmente conocidos son, por ejemplo, Youtube, Messenger, Skype y Facebook que proporcionan herramientas de comunicación, compartición de vídeos, música, fotos, chats, etc… cada vez más usadas. Las nuevas tendencias hacen que la sociedad tenga nuevas necesidades que cubrir, por lo que hace que estas redes de comunicaciones y su funcionamiento interno se deba ir adaptando a los cambios que se van produciendo y además ir previendo la tendencia de cara al futuro.

Actualmente las personas se mueven continuamente por todo el mundo, y en todo momento les gusta poder consultar su correo, enviar fotos, vídeos, hacer reserva de viajes, surfear por la web, etc. Todo esto ha sido posible gracias a la integración y convergencia de las redes inalámbricas móviles, con las cuales se pretende proporcionar servicios de datos de alta velocidad, QoS, seguridad y movilidad en ambientes de banda ancha. Para satisfacer la demanda de estas aplicaciones emergentes los operadores móviles deben migrar a infraestructuras de red más ricas que permitan reunir los diversos requerimientos que precisan estas aplicaciones emergentes. Como es de suponer, la creación de este nuevo ambiente incrementará su complejidad, y en este contexto, la gestión de red es un factor crucial en el éxito del ofrecimiento de nuevos servicios.

Dentro del proceso de gestión, la tarificación es una actividad clave que junto con autenticación, autorización, y la facturación determinan los elementos funcionales esenciales en la cadena de generación de valor del operador de red. Sin embargo, los modelos de tarificación usados en las redes de telecomunicaciones y datos han sido bastante simples. Los usuarios son facturados con una tarifa plana, basada en sus suscripciones. La suscripción es el contrato entre el proveedor del servicio y un cliente y es conocido como “Acuerdo de Nivel de Servicio” (SLA – Service Level Agreement). La idea de un SLA dinámico permitirá que una serie de parámetros puedan ser modificados de acuerdo al comportamiento de la red y la interacción de la información de retroalimentación de eventos relacionados al nivel de servicio requerido. Sin embargo ésta flexibilidad introduce algunas dificultades al proceso de tarificación. Nuevos mecanismos de tarificación, recolección de información de eventos tarificables y modelos de facturación son necesarios. Como resultado de la migración de SLA estático a dinámico, el interés crecerá para cambiar de un modelo de tarifa plana hacia modelos de cobro basado en uso o en eventos.

La arquitectura de gestión de red tradicional es simple y centralizada con énfasis en el monitoreo más que en el control. La gestión de red debe cumplir con requerimientos de gestión adicional, similar a los modelos de servicio de negocio de las redes de hoy: diferenciación de servicio, personalización de servicio, negociación dinámica de servicios, mayores características y flexibilidad. Durante los últimos años, la gestión basada en políticas ha sido un objeto de investigación, como una alternativa sencilla

para el proceso de gestión de redes. La simplificación y automatización del proceso de gestión de red es una de las aplicaciones claves del sistema de políticas.

Como consecuencia del análisis de requerimientos de esta nueva red, se propone una arquitectura basada en políticas para la gestión de la tarificación. Para ello, y partiendo como base de la arquitectura y las características básicas de UMTS, así como teniendo en cuenta también la autenticación, la movilidad y los traspasos, se plantea una arquitectura para un escenario global. Dentro de esta arquitectura, y para este escenario global se proponen una serie de entidades que compondrán la arquitectura y se definen las funciones de cada entidad.

Se entra más en detalle con la arquitectura diseñada y se analizan los diferentes escenarios posibles en los cuales nos podemos encontrar. Con ello se establece el escenario general que se implementará y se utilizará en las simulaciones para evaluar el rendimiento del diseño en los diferentes modos de operación de la red. Se plantea un protocolo para analizar el comportamiento de la arquitectura en el escenario general, teniendo en cuenta cada una de las fases y modelos de señalización posibles.

Como resultado, se han configurado los modelos, teniendo en cuenta unos parámetros de tráfico, retardos de propagación, retardos de transmisión de datos y retardos de procesado determinados y se han hecho simulaciones donde se han evaluado la influencia de las variaciones de diferentes variables correspondientes a la arquitectura, como son la velocidad de las líneas de señalización, a la naturaleza del tráfico entrante, como son el tipo de petición (traspaso o nuevo servicio) y la tasa de entrada, al estado y configuración de la red, como son el tipo de autenticación utilizado (serie o paralelo), teniendo en cuenta la ocupación de las celdas mediante un algoritmo de selección de celda escoger la óptima para satisfacer el servicio, y finalmente a la procedencia de la conexión, si está o no conectado inicialmente con su Home Operator.

Finalmente, mediante el análisis de los resultados se constata que tanto el empleo de la autenticación en paralelo como el aumento de la velocidad de las líneas de señalización son claves en la mejora considerable de los retardos que se producen en la señalización. En el caso de la autenticación en paralelo perdemos un poco de seguridad en general, porque se permite momentáneamente al usuario del acceso a unos servicios que aún no se sabe con certeza si tendrá acceso, pero el pequeño riesgo merece la pena en cuanto a la reducción del número de mensajes enviados hasta proporcionarle servicio al usuario.

En el caso del aumento de la velocidad de las líneas de señalización, aparte de reducirse drásticamente el retardo global en la atención de las peticiones, se consigue solucionar un problema de desincronización que había en la actualización de la información de los recursos disponibles de la red y que hacía que el algoritmo de selección de celda actuará de forma errónea. Con líneas más lentas se producían gran cantidad de peticiones rechazadas en la entidad que no le correspondía. La causa era la lentitud de la llegada de la información de actualización de la disponibilidad de recursos de la red. Esto afectaba en mayor medida a las peticiones de traspaso atendidas, lo cuál hacía que las peticiones de nuevo servicio tuvieran cierta ventaja ante las de traspaso, hecho que no debería suceder. Afortunadamente, el hecho de aumentar la velocidad de las líneas de señalización solventa este problema.

ÍNDICE

Introducción

Con la integración y convergencia de las redes inalámbricas móviles se pretende proporcionar servicios de datos de alta velocidad, calidad de servicio (QoS – Quality of Service), seguridad y movilidad en ambientes de banda ancha. La migración a una infraestructura de red más rica (en términos de características) permite a los operadores móviles reunir los requerimientos diversos de la demanda de aplicaciones emergentes. No obstante, la creación de este nuevo ambiente incrementará su complejidad. En este contexto, la gestión de red es un factor crucial en el éxito del ofrecimiento de nuevos servicios.

Dentro del proceso de gestión, la tarificación es una actividad clave que junto con autenticación, autorización, y facturación determinan los elementos funcionales esenciales en la cadena de generación de valor de un operador de red. Sin embargo, los modelos de tarificación usados en las redes de telecomunicaciones y datos han sido bastante simples. Los usuarios son facturados con una tarifa plana, basada en sus suscripciones. La suscripción es el contrato entre el proveedor del servicio y un cliente y es conocido como "Acuerdo de Nivel de Servicio" (SLA – Service Level Agreement). La idea de un SLA dinámico permitirá que una serie de parámetros puedan ser modificados de acuerdo al comportamiento de la red y la interacción de la información de retroalimentación de eventos relacionados al nivel de servicio requerido. Sin embargo ésta flexibilidad introduce algunas dificultades al proceso de tarificación. Nuevos mecanismos de tarificación, recolección de información de eventos tarificables y modelos de facturación son necesarios. Como resultado de la migración de SLA estático a dinámico, el interés crecerá para cambiar de un modelo de tarifa plana hacia modelos de cobro basado en uso o en eventos.

La arquitectura de gestión de red tradicional es simple y centralizada con énfasis en el monitoreo más que en el control. La gestión de red debe cumplir con requerimientos de gestión adicional, similar a los modelos de servicio de negocio de las redes de hoy: diferenciación de servicio, personalización de servicio, negociación dinámica de servicios, mayores características y flexibilidad. Durante los últimos años, la gestión basada en políticas ha sido un objeto de investigación, como una alternativa sencilla para el proceso de gestión de redes. La simplificación y automatización del proceso de gestión de red es una de las aplicaciones claves del sistema de políticas.

I. Ámbito del proyecto

El ámbito en el que se encuadra el siguiente proyecto es en un sistema de comunicaciones móviles avanzado. Siguiendo las bases de la arquitectura UMTS se determinan las nuevas entidades a diseñar dentro de una arquitectura más compleja de gestión de la tarificación, la cual deberá cumplir con los requerimientos de nuevos mecanismos de tarificación, recolección de información de eventos tarificables y modelos de facturación.

Posteriormente, al hablar de movilidad se analizan los diferentes escenarios que surgen, se describen los diferentes tipos de traspasos que pueden ocurrir, se determinan los

parámetros críticos de cada uno, y se diseñan los protocolos más adecuados para cada caso.

Finalmente se estudia en detalle el escenario más complejo y se analiza la influencia de las variaciones de los diferentes parámetros de diseño y niveles de carga del sistema en el correcto devenir del protocolo propuesto dentro de la arquitectura diseñada.

II. Declaración de objetivos

El presente proyecto tiene como objetivo el diseño e implementación de una arquitectura basada en políticas para la gestión de la tarificación dentro de un ambiente de comunicaciones móviles avanzado.

Concretamente, los objetivos consistirán en el desarrollo de las siguientes tareas:

- Diseñar la arquitectura de gestión de la tarificación para un entorno de red de comunicaciones móviles avanzado.
- Diseñar la arquitectura basada en políticas para control del proceso de tarificación.
- Implementar los componentes de las arquitecturas diseñadas.
- Analizar el rendimiento de las arquitecturas dentro del ambiente de comunicaciones móviles avanzado.

III. Estructura del proyecto

La estructura del proyecto final de carrera está formada por una serie de 4 capítulos, conclusiones y anexos. En el capítulo 1 se describe la arquitectura, las características básicas y las funciones de la red UMTS, además se introducen conceptos generales acerca de autenticación, redes basadas en políticas, movilidad y traspasos y finalmente tarificación.

En el capítulo 2, se enumeran los requerimientos generales de la arquitectura a diseñar, se evalúa el escenario global y se definen las entidades que incorporará la arquitectura, así como las funciones generales de cada una estas entidades propuestas.

En el capítulo 3, se analizan detenidamente los posibles escenarios en que se puede encontrar la arquitectura, determinando las peculiaridades de cada uno de ellos. Se define un escenario de simulación, el cual se utilizará en las simulaciones para evaluar el rendimiento del diseño. Se define el flujo de señalización en cada acción que se deba ejecutar dentro de la arquitectura y finalmente se definen los parámetros utilizados en la simulación.

En el capítulo 4 se muestran y se estudian los resultados obtenidos en las simulaciones. Se obtienen las variaciones del retardo promedio de traspasos, retardo promedio de nuevos servicios y porcentaje de peticiones rechazadas en función del valor de otras variables independientes que controlamos externamente para evaluar como se comporta la arquitectura. Estas variables que controlamos externamente son la tasa de llegadas, la

velocidad de la línea de señalización, el tipo de autenticación utilizado (serie o paralelo), etc.

Finalmente, se introduce un capítulo de conclusiones y se añaden unos anexos para complementar con más detalle el contenido de la memoria.

IV. Siglario

3GPP	3rd Generation Partnership Project
AA	Autenticación y Autorización
AAA	Authentication, Authoritzation & Accounting
API	Application Program Interface
AVP	Attribute Value Pairs
BER	Bit Error Rate
BW	Bandwidth
CC	Charging Control
COPS	Common Open Policy Service
CT	Contenedor de información de Tarificación
FDDI	Fiber Optics Data Distributed Interface
FGT	Función de Gestión de la Tarificación
FU	Ficha de Usuario
GSM	Global System for Mobile Communications
HO	Home Operator
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LADP	Lightweight Directory Access Protocol
ME	Mobile Equipment
MT	Mobile Termination
NAS	Network Access Server
NED	Network Description
PAS	Policy Administration System
PBN	Policy-based Network
PDA	Personal Digital Assistant
PDF	Policy Decision Function
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMS	Policy Management System
PR	Policy Recipient
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Server
RAN	Radio Access Network
RAT	Radio Access Technology
SIP	Session Initiation Protocol

SLA	Service Level Agreement
SM	Sonda de Medición
SNMP	Simple Network Management Protocol
TE	Terminal Equipment
TLS	Transport Layer Security
TU	Terminal de Usuario
UCP	User Connection Profile
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
USIM	User Service Identity Module
VASP	Value-Added Service Provider
VO	Visitor Operator
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XML	extensible Marcus Language

1 Conceptos generales

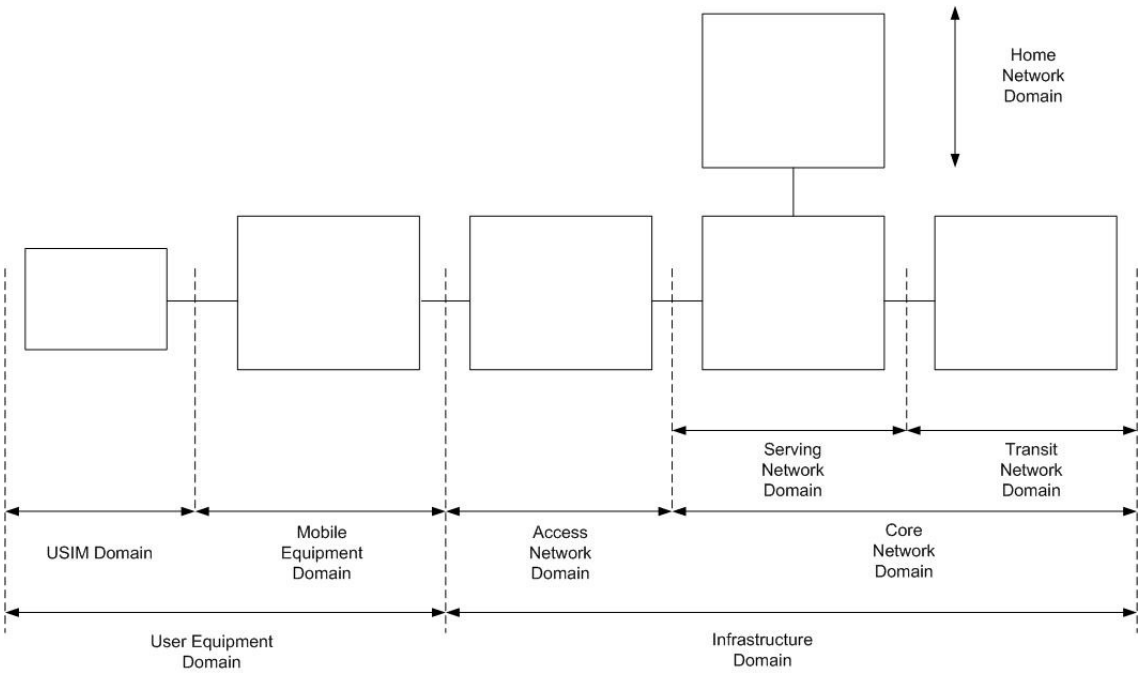
Previamente a entrar de lleno en el proyecto en sí, se establecen las bases de conocimiento previos abordando de manera superficial diferentes conceptos básicos sobre UMTS (Universal Mobile Telecommunication System), autenticación, gestión de políticas y traspasos.

1.1 UMTS – Arquitectura, características básicas, funciones,…

En alto nivel, la arquitectura general de UMTS [1] es modelada tanto por el punto de vista físico como por el funcional, aunque por motivos de utilidad en el posterior trabajo realizado y por simplicidad en la lectura sólo se explicará por encima el punto de vista físico. En este caso, los aspectos físicos serán modelados usando el concepto de dominio.

Dominios en UMTS

La siguiente figura muestra los dominios básicos de UMTS tal y como serán descritos en este apartado.



NOTA: En cuanto a los dominios, se ha mantenido la nomenclatura inglesa usada en las especificaciones del 3GPP (3rd Generation Partnership Project) para no crear divergencias.

Los dominios identificados en la figura resultaran de la evolución de infraestructuras de red ya existentes, como bien podría ser GSM (Global System for Mobile Comunications) o similares.

Figura 2.1 – Dominios UMTS

1.1.1 División de dominios

En cuanto a la arquitectura básica se suele hacer una división entre los terminales de usuario y la infraestructura. Lo cual resulta en dos dominios diferentes: el dominio de los terminales de usuario o *'User Equipment Domain'* y el dominio de infraestructura.

En cuanto a los terminales de usuario se entiende como los equipos usados por los usuarios para acceder a los servicios UMTS, ya sea un teléfono móvil, una PDA (Personal Digital Assistant), un portátil o cualquier otro equipo que pueda acceder a la red. Estos equipos disponen de un interfaz radio para acceder a la infraestructura. Al hablar de infraestructura nos referimos a los nodos físicos que realizan las funciones requeridas para poner fin al interfaz radio y soportar los requerimientos de los servicios de telecomunicaciones que se ofrecen al usuario final. La infraestructura es un recurso compartido que proporciona servicio a todos los usuarios finales autorizados dentro del área de cobertura.

1.1.2 Terminal de usuario – User Equipment Domain

Este dominio abarca una alta variedad de dispositivos con diferentes niveles de funcionalidad, los cuales pueden ser compatibles con uno o más interfaces de acceso (fijo o radio) como por ejemplo los terminales de modo dual UMTS-GSM. Los terminales pueden incluir una tarjeta inteligente extraíble que puede ser usada en diferentes dispositivos. El dominio de terminales de usuario es a su vez subdividido en dos dominios más: el dominio de Equipo Móvil (*ME – Mobile Equipment Domain*) y el Módulo de Identidad de Servicios de Usuario (*USIM – User Services Identity Module Domain*).

Equipo Móvil – ME

El equipo móvil realiza la transmisión radio y contiene las aplicaciones que utiliza el terminal. El equipo móvil es a su vez subdividido en varias entidades, una que realiza la transmisión radio y funciones relacionadas, Terminación Móvil (*MT – Mobile Termination*), y otra que contiene las aplicaciones extremo a extremo, Equipo Terminal (*TE – Terminal Equipment*).

Módulo de Identidad de Servicios de Usuario – USIM

El USIM contiene datos y procedimientos los cuales le identifican sin ambigüedad y de forma segura. Estas funciones están típicamente incluidas en una tarjeta inteligente autónoma. Este dispositivo está asociado a un usuario en concreto, y como tal permite la identificación del usuario independientemente del equipo móvil que utilice.

En la imagen inferior se muestra el modelo funcional para el terminal de usuario, UE (User Equipment).

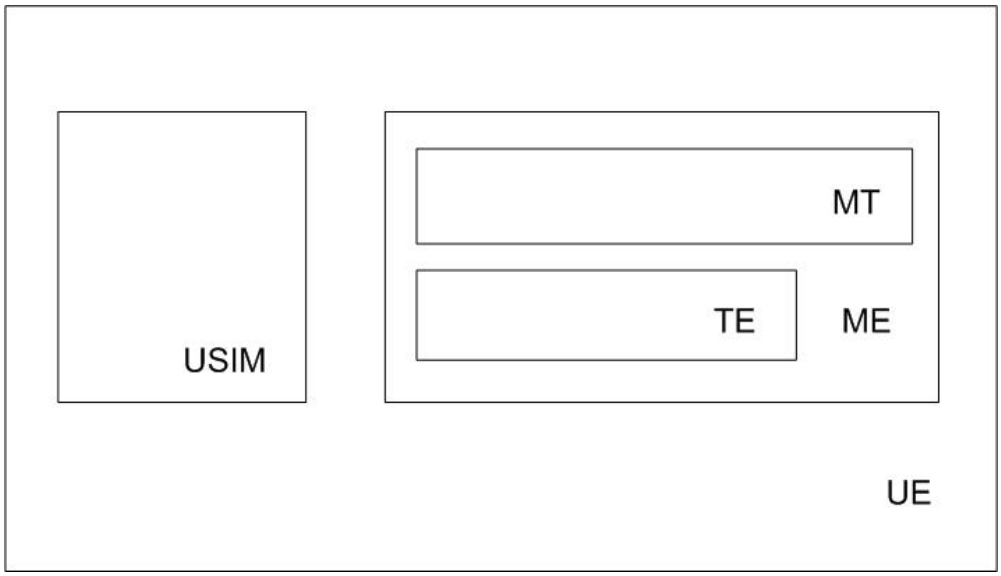


Figura 2.2 – Modelo funcional del terminal de usuario

1.1.3 Dominio de Infraestructura – Infrastructure Domain

El dominio de infraestructura está a su vez subdividido en el dominio de red de acceso (*Access Network Domain*), el cuál se caracteriza por estar en contacto directo con el terminal de usuario y el dominio de núcleo de red (*Core Network Domain*). Esta división pretende simplificar y ayudar al proceso de desemparejar las funcionalidades relacionadas con el acceso y las no relacionadas con el mismo y está en línea con el principio modular adoptado por UMTS.

El dominio de acceso de red se compone por encima de las funciones específicas de la técnica de acceso, mientras que las funciones en el dominio de núcleo de red pueden ser potencialmente usadas con flujos de información usando cualquier técnica.

Dominio de red de acceso

El dominio de red de acceso consiste en entidades físicas que gestionan los recursos de la red de acceso y proporcionan al usuario un mecanismo para acceder al dominio de núcleo de red.

Dominio de núcleo de red

El dominio de núcleo de red consiste en entidades físicas que proporcionan soporte a las características de red y a los servicios de telecomunicaciones. El soporte proporcionado incluye funcionalidades tales como la gestión de la información de localización del usuario, el control de las características y servicios de la red, los mecanismos de

transferencia (conmutación y transmisión) para la señalización y para la información generada por el usuario.
El dominio del núcleo de red se subdivide en el dominio de red de servicio (*Serving Network Domain*), el dominio de red en casa (*Home Network Domain*) y el dominio de red de tránsito (*Transit Network Domain*).

Dominio de red de servicios

El dominio de red de servicios es la parte del dominio del núcleo de red al que es conectado el dominio de red de acceso que proporciona el acceso del usuario. Éste representa las funciones del núcleo de red que son locales al punto de acceso del usuario y por lo tanto cambia su localización cuando el usuario se mueve. El dominio de red de servicios es responsable del enrutamiento de las llamadas y el transporte de los datos del usuario desde su origen hacia su destino. Éste tiene la habilidad de interaccionar con el dominio de casa para satisfacer datos o servicios específicos al usuario y con el dominio de tránsito para otros propósitos que no corresponden al usuario.

Dominio de red en casa

El dominio de red en casa representa las funciones del núcleo de red que son llevadas a cabo en una localización permanente sin tener en cuenta la localización del punto de acceso del usuario.

El USIM es relacionado mediante suscripción al dominio de red en casa. El dominio de red en casa por lo tanto contiene por lo menos permanentemente datos específicos de usuario y es responsable de la gestión de la información de suscripción. También puede ocuparse de servicios específicos, potencialmente no ofrecidos por el dominio de red de servicios.

Dominio de red de tránsito

El dominio de red de tránsito es la parte del núcleo de red localizado en el camino de comunicaciones entre el dominio de red de servicios y la parte remota. Si, para una llamada dada, la parte remota está localizada dentro de la misma red que el terminal de de usuario que la origina, entonces no se activa ninguna instancia particular en el dominio de tránsito.

1.2 Autenticación – Visión general

Ciertas aplicaciones comparten la necesidad de autenticarse mutuamente entre el cliente (p.e terminal móvil) y un servidor de aplicaciones antes de que la comunicación pueda llevarse a cabo. Como ejemplo se podría mencionar la comunicación entre un cliente y un servidor de presencia, comunicaciones con portales de infraestructura de clave pública donde el cliente solicita un certificado digital, comunicaciones con un servidor de contenidos móvil broadcast/multicast, etc.

Generalmente hablando hay dos tipos de mecanismos de autenticación [2]. Uno basado en una clave compartida entre las entidades que se comunican, y otro basado en pares de clave pública y privada y certificados digitales.

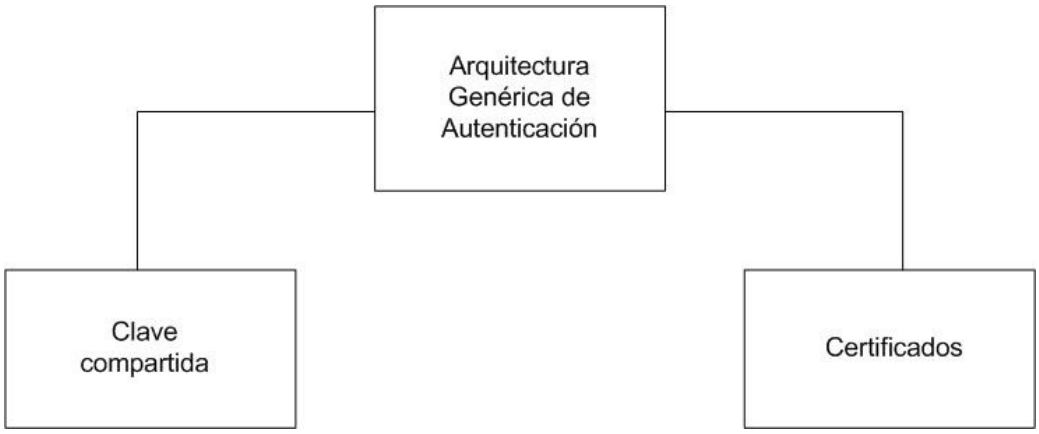


Figura 2. 3 – Visión general de la arquitectura genérica de autenticación

1.2.1 Autenticación usando clave compartida

Hay varios protocolos de autenticación que confían en una clave pre-compartida entre las dos entidades comunicantes. Ejemplos conocidos son http (Hypertext Transfer Protocol) Digest, Pre-Shared Key TLS (Transport Layer Security), IKE (Internet Key Exchange) con clave pre-compartida y cualquier otro mecanismo basado en un nombre de usuario y una contraseña.

El principal problema con estos mecanismos es como ponerse de acuerdo para la clave compartida. Para más información acerca de cómo se soluciona este problema en un contexto móvil, se deja como referencia la siguiente especificación técnica [3] ya que no se profundizará más sobre el tema.

1.2.2 Autenticación basada en pares de clave pública y privada y certificados

Una alternativa a usar claves compartidas para la autenticación es mediante el uso de criptografía asimétrica. Este método asume que la entidad que necesita ser autenticada (una o ambas partes en la comunicación) posee un par de claves pública y privada y su correspondiente certificado digital. Este último valida el par de claves y asocia este par de claves con su legítimo propietario.

La principal desventaja de este tipo de autenticación es que se necesita una infraestructura de clave pública y que el hecho de tener que realizar operaciones criptográficas con clave asimétrica a menudo requiere un coste computacional sustancialmente mayor que las operaciones con clave simétrica.

En la especificación técnica [4] se puede encontrar más información acerca de cómo un operador móvil puede expedir certificados digitales para sus suscriptores.

1.2.3 Directrices para el uso de la arquitectura genérica de autenticación

Dependiendo de la configuración de la red y de las políticas del operador, un servidor de aplicaciones o un proxy de autenticación estarán capacitados para usar cualquiera de las alternativas proporcionadas por la arquitectura genérica de autenticación o incluso cualquier otro mecanismo de autenticación de usuario especificado fuera del 3GPP si tal mecanismo está a su disposición.

Esta sección trata de dar una visión general de los argumentos que juegan un papel importante en el momento de escoger un mecanismo de autenticación. El mecanismo de autenticación seleccionado dependerá de:

1. Requerimientos y políticas relacionadas con el usuario, servidor, aplicación o dispositivo que necesita autenticación. Esto puede ser en ambas direcciones (autenticación mutua), aunque usualmente se enfatiza en la autenticación del usuario hacia el servidor.
2. Dispositivo y características del servicio, capacidades de usuario y preferencias definidas en el perfil de usuario.
3. Políticas de la red o de las redes que proporcionan el servicio de transporte y de los servidores que proporcionan las aplicaciones.

Los requerimientos y las políticas de autenticación dependerán de si existe la necesidad de:

a) **Autenticación de dispositivo:** El dispositivo es genuino y no un clon. Autenticación de la tarjeta SIM.

b) **Protección de la integridad:** Un ejemplo sería la debilidad en el acceso a GSM, el cuál permitiría a una persona situada en medio de la comunicación manipular de forma fácil los mensajes de señalización. Un forma de prevenir esto sería usando autenticación de dispositivos y protección de la integridad vía código de autenticación de mensaje mediante clave en los mensajes específicos de señalización.

c) **Autenticación de aplicación:** Esto sería a menudo necesario para comprobar la autenticidad de las aplicaciones de software.

d) **Autenticación de usuario:** Esto hace referencia a la autenticación del usuario final, la persona que está usando el dispositivo de usuario final. Una forma de

hacer esto sería mediante la disponibilidad del USIM para dispositivos, protocolos y aplicaciones dependiendo, lógicamente, de la entrada por parte del usuario de un número de identificación personal (PIN – Personal Identification Number), o físicamente mediante una política de extracción e inserción. La entrada de un PIN puede ser también requerida antes de que el acceso a una aplicación específica sea permitido.

e) **Autenticación de transacción y de no repudio:** Para varias transacciones de negocios que se llevan a cabo usando dispositivos móviles es necesario firmar digitalmente la transacción con claves privadas de usuario, específicamente cuando hay una necesidad de no repudio como por ejemplo para prevenir:

- La falsa negación del envío del mensaje
- El contenido del mensaje
- El momento del envío del mensaje

NOTA: Muchas técnicas de autenticación están basadas en una clave única que es compartida entre la red y el usuario – esto está bien para la autenticación del remitente y el destinatario, pero el no repudio probable por una tercera parte puede requerir el uso de técnicas de clave pública dónde la clave privada pertenece sólo al remitente.

Uso de clave compartida

Algunos ejemplos donde se utiliza la clave compartida son:

- distribución de claves simétricas de cifrado y de integridad para aplicaciones de securización que corren entre el terminal de usuario y el servidor en la red;
- distribución de contraseñas y PIN para aplicaciones externas;
- para proteger la distribución de certificados entre los terminales de usuario y la autoridad certificadora.

Uso de certificados

Algunos ejemplos donde los certificados se utilizan para la autenticación son:

- cuando es necesario comprobar la identidad del usuario final;
- cuando el protocolo de seguridad de la aplicación trabaja con autenticación de par de claves públicas y privadas y el suscriptor dispone de certificado;
- donde hay una necesidad de no repudio y donde el usuario requiere firmar digitalmente una transacción con una clave privada de usuario.

1.3 Redes basadas en políticas – PBN

Policy-based Network (PBN) es un método independiente para facilitarle al administrador la operación de redes basadas en IP (Internet Protocol) e introducir el concepto de control dinámico. En este tipo de arquitectura el comportamiento del sistema es especificado por reglas de políticas de alto nivel y no por configuraciones explícitas de elementos del sistema individuales como en las redes tradicionales.

Las políticas son los enlaces entre una especificación de servicio deseado de alto nivel y configuraciones de los elementos de red que proporcionan esos servicios. Las políticas pueden manejar configuración de red, incluyendo QoS, SLAs, Virtual Private Network (VPN), y problemas de seguridad.

Un sistema de gestión de políticas (PMS – Policy Management System) está formado por una serie de componentes funcionales (Figura 2.4):

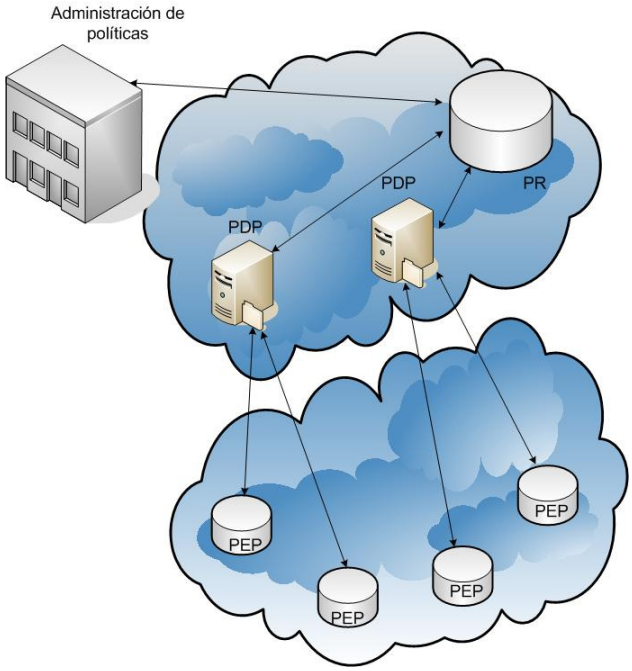


Figura 2.4 – Componentes de la red PBN

Todas las políticas son almacenadas en un contenedor de políticas (PR – Policy Recipient), las cuáles son definidas y administradas mediante un sistema de administración de políticas (PAS – Policy Administration System). El punto de decisión de políticas (PDP – Policy Decision Point), el cual es conocido como Policy Decision Function (PDF) por el 3GPP, se comunica con el contenedor de políticas mediante el protocolo LADP (Lightweight Directory Access Protocol) [5] para recuperar las políticas necesarias para dar respuesta a las peticiones realizadas por el punto de imposición de políticas (PEP – Policy Enforcement Point), la comunicación entre el PDP y el PEP es llevada a cabo mediante el protocolo Common Open Policy Service (COPS) [6].

1.4 Movilidad y traspasos

En el futuro de las telecomunicaciones habrá una gran convergencia de redes heterogéneas. Esta red se visualiza como ambientes de comunicaciones dinámicas, donde una multitud de diferentes dispositivos inalámbricos, tecnologías de acceso radio, y operadores de red podrán cooperar o competir mediante acuerdos de cooperación instantáneos.

Los pasos de integración de las tecnologías de radio heterogéneas hacia un ambiente de acceso multiradio ha sido tomado por cuerpos de estandarización y operadores comerciales. Esta integración abre un camino potencial para acceder a cualquier red proporcionándole al usuario el modelo de "always best experience" y "always best connected". Además abre la posibilidad para el usuario de ser servido vía diferentes puntos de acceso de servicio, posiblemente perteneciendo a diferentes redes de acceso radio (RAN – Radio Access Network) implementadas por diferentes tecnologías de acceso radio (RAT – Radio Access Technology) y operadas por diferentes operadores. Además de esto, el mantenimiento de la continuidad de servicio y la movilidad para usuarios intercambiando entre accesos requiere soporte de traspaso (handover) entre diferentes RATs, soporte para cooperación entre las diferentes RANs y soporte para el rápido establecimiento de acuerdos roaming (dinámicos).

Para proporcionar a los usuarios los servicios sin importar su localización, las diferentes redes tendrán que colaborar. En un ambiente altamente móvil, la colaboración entre las redes tendrá que hacerse "sobre la marcha". Dos ventajas importantes de este nuevo ambiente son:

1. Incremento en la disponibilidad y calidad del servicio al usuario a bajos costos de producción comparados con las redes actuales.
2. Reduce las barreras de entrada para nuevos actores en el mercado del mundo de las redes inalámbricas.

El incremento en la disponibilidad del servicio se debe a que con más frecuencia tendremos la disponibilidad de acceso en más localizaciones. Mejor calidad de servicios no solo es el resultado de la disponibilidad de mayor número de accesos, sino además de la mejora para el manejo rápido y eficiente de recursos de accesos heterogéneos lo cual da como resultado una mejor experiencia de servicio transparente.

La segunda ventaja es que reducirá las barreras de entrada de la industria inalámbrica, enfocándose en una estructura de mercado más competitiva e innovadora.

En el futuro, el número y la diversidad de redes de acceso y operadores se incrementará notablemente. Por ejemplo: Los hotspot WLAN (Wireless Local Area Network) serán más difundidos debido a la fácil y relativamente económica implementación. Estos hotspots serán operados como parte de una red o individualmente. Con este ambiente algunas tareas serán esenciales, por ejemplo, la necesidad de ser anunciados los recursos (la existencia y la oferta) desde las diferentes redes heterogéneas, buscar y evaluar las ofertas de red y seleccionar "la mejor red". Es aquí donde surge una pregunta importante, ¿cuál es la mejor red? "La mejor red puede ser seleccionada con respecto al desempeño, preferencias del usuario, costo, y requerimientos de servicio. Además de esto, varias redes podrían ser seleccionadas al mismo tiempo, con lo cual se permitiría

elegir entre diferentes rutas para desempeñar un balanceo de carga, enriqueciendo la confiabilidad de una conexión, o reaccionar a cambios en la topología.

1.5 Tarificación

Debido a la presión para el soporte de desarrollos rápidos y cambios en las relaciones de negocio, los proveedores de servicios están encarando grandes retos con respecto a la tarificación de servicios en tiempo real. Aunado a eso, el interés está creciendo para un cambio de tarifa plana hacia un evento de cargo basado en tiempo o uso, el cual introduce una complejidad adicional a la gestión de la tarificación. Esto ha creado una lista de requerimientos que las nuevas arquitecturas deben cumplir.

- Desde el punto de vista del usuario, la principal demanda es la provisión "One stop Billing", es decir, una sola factura por los servicios de voz y datos ofrecidos por los operadores de red y proveedores de servicios independientes. Otro requisito es la negociación dinámica de nivel de servicio que se adapte a sus necesidades.
- Desde el punto de vista del operador el requerimiento es una arquitectura de tarificación genérica que cubra los diferentes modelos de cobro (tiempo, volumen, basado en QoS, tarifa plana, por conteo, etc.) Por otro lado, el soporte de los mecanismos de cargo existentes (prepago, postpago).

Además, la alta movilidad del usuario a través de los diferentes dominios y tecnologías incrementará la complejidad de la tarificación y la seguridad del proceso. Una de las alternativas de gestión es el modelo basado en políticas, el cual se ha explicado anteriormente. Este modelo permite la configuración dinámica de los dispositivos, con lo cual permite adaptarse a los requerimientos de nivel de servicio dinámico.

1.5.1 Arquitectura

La arquitectura está formada por una estructura jerárquica de servidor AAA (Authentication, Authorization and Accounting) que se pueden encontrar ubicados en diferentes partes de la red o en diferentes dominios, dependiendo del papel a desempeñar durante el proceso de tarificación. Tres roles pueden ser desempeñados por los servidores AAA.

- **Principal AAA:** Es el servidor que se localiza en el dominio del operador del usuario (Home Operator) y es el que autentica y autoriza al usuario. Además es el responsable de coordinar el proceso de tarificación del usuario.
- **Proxy AAA:** Es el servidor que se encuentra en la red de acceso, en la cual el usuario se encuentra conectado. Este servidor cambiará conforme el usuario se mueve de una red de acceso a otra.
- **Externo AAA:** Es el servidor que se encuentra en los proveedores de servicio de valor añadido y que realizan la recopilación de información y generan su propio cobro por el servicio ofrecido al usuario.

Por su parte, los elementos de servicio son los que proporcionan diferentes tipos de servicios en la red. Algunos de ellos participan activamente en la provisión del servicio

y el usuario tiene el conocimiento de su existencia, por ejemplo, un servidor web. Otros no son visibles al usuario, pero son necesarios en el proceso de provisión del servicio, por ejemplo routers o medidores de tráfico.

El controlador de políticas es un servidor que almacena, controla y envía a los equipos las políticas específicas de acuerdo a las tareas desempeñadas. Las políticas son clasificadas en tres niveles:

Nivel de políticas	Ejemplo de políticas
Cobro y facturación	Definición de tipos de pago, forma de facturación, tiempo de facturación
Tarificación	Forma de tarificación, reglas de generación, transporte y almacenaje de datos de tarificación
Medición	Alcance de la medición, atributos de los flujos de medición, granularidad del flujo

El equipo del usuario puede realizar la negociación de nivel de servicio mediante la implementación del modelo de políticas. Esta negociación tendrá impacto en las configuraciones de los equipos.

1.5.2 Protocolos de AAA

Diferentes protocolos en soporte de AAA han sido discutidos dentro del IETF (Internet Engineering Task Force). Los protocolos de mayor relevancia en el contexto de AAA son: RADIUS (Remote Access Dial-In User Server), Diameter, COPS y SNMP (Simple Network Management Protocol).

RADIUS [7] [8] fue creado para transmitir datos de autenticación y autorización entre un servidor de acceso de red, el cual es visto como cliente RADIUS y un servidor RADIUS que tiene la información del usuario a autenticar. Existen extensiones para entregar información de accounting básica (inicio, final y actividad de datos) a un servidor accounting de RADIUS. Algunas de las deficiencias que tiene RADIUS son el tamaño limitado de atributos de datos, el control de sesión limitado para ser usado en accounting y la baja tolerancia a fallos debido al uso UDP (User Datagram Protocol).

El protocolo DIAMETER [9] fue definido como el sucesor de RADIUS. El protocolo satisface los requerimientos de acceso de red haciendo uso de diferentes tecnologías de acceso, incluyendo tecnologías inalámbricas y modelos de seguridad distribuidos para escenarios de roaming y multidominio. Está formado por una base que define encabezados y extensiones de seguridad y un número de comandos y atributos de pares de valores (Attribute Value Pairs). Extensiones Mobile IP definen AVPs para soportar Mobile IP a través de dominios administrativos diferentes. Esto permite llevar a cabo las funciones AAA para un equipo móvil. La extensión de tarificación define un conjunto de AVPs de accounting genérico que puede ser usado para todos los servicios y soporta accounting en tiempo real.

El protocolo COPS permite el intercambio de información de políticas entre un PDP y un PEP. Es un protocolo del modelo cliente/servidor. Ha sido especificado para permitir

autorización de peticiones de reserva de recursos en redes soportando servicios integrados.

2 Arquitectura planteada

Con la integración y convergencia de las redes inalámbricas móviles se pretende proporcionar servicios de datos de alta velocidad, QoS, seguridad y movilidad en ambientes de banda ancha. Este nuevo ambiente es visualizado como una solución de integración de red a los problemas de los días modernos de conmutación de una red a otra para conservar el contacto con el mundo exterior. El ambiente es visto como una red que deriva de las tecnologías existentes y emergentes para la entrega de múltiples servicios.

Este ambiente conceptualiza que los usuarios podrán beneficiarse en varias formas de esta plataforma de acceso unificado. La arquitectura demanda clientes móviles adaptables y flexibles que se puedan enfrentar con diversos ambientes dinámicos y heterogéneos. Los usuarios tendrán acceso a redes inalámbricas sin importar la tecnología o el dominio administrativo, y serán capaces de acceder a una variedad de servicios proporcionados por sus operadores o por proveedores independientes sin ningún contrato adicional. Estas características involucrarán muchas modificaciones en los modelos de gestión y provisión de servicios actuales. Cuestiones desafiantes e importantes relacionadas a arquitecturas, acceso multiradio, modelos de tarificación, gestión de red, redes con conocimiento de contexto, movilidad, etc., tienen que ser contestadas.

2.1 Requerimientos generales

Los requerimientos generales están relacionados con los problemas a los que las redes de acceso tienen que hacer frente, los cuales enumeraremos a continuación:

1. **Redes Heterogéneas:** La arquitectura soportará diferentes tipos de tecnologías para proporcionar a los usuarios la conectividad óptima según sus requerimientos y preferencias.
2. **Movilidad:** Las redes de acceso deben soportar esquemas de gestión de movilidad para usuarios, servicios, sesiones, terminales y movilidad de red. Debe ofrecer a las redes la flexibilidad de moverse a diferentes localizaciones físicas y lógicas en cualquier momento.
3. **Composición:** La arquitectura de red soportará mecanismos para alcanzar negociaciones y acuerdos “al vuelo” a través de diferentes dominios administrativos.
4. **Seguridad y privacidad:** Las redes de acceso deben proporcionar un esquema de seguridad flexible, comprensiva y transparente que opere consistentemente a través de un ambiente cambiante de redes heterogéneas. También es importante establecer una relación de confianza entre las diferentes redes que se comuniquen o compongan. Tres tipos de relaciones de confianza han sido identificados: confianza directa, confianza dividida y no confianza.
5. **Migración y compatibilidad:** Las redes de acceso deben soportar los mecanismos y caminos de migración de las redes y terminales móviles existentes
6. **Robustez y tolerancia a fallos de red:** La arquitectura de red y la gestión de red deben permitir la construcción de redes que sean escalables, robustas,

confiables, con alta disponibilidad y supervivencia a través de redes heterogéneas en ambientes cambiantes dinámicamente.

7. **Calidad de servicio:** Deben proporcionar las capacidades para ofrecer múltiples clases de QoS para servicios extremo a extremo, a través de diferentes tipos de tecnologías de red y diferentes direcciones de dominio. También deben de proporcionar negociaciones "al vuelo" para cambiar clases de QoS desde el lado del usuario o de la red.
8. **Soporte multidominio:** La arquitectura debe soportar de forma transparente funcionalidad de red abarcando diferentes dominios administrativos.
9. **Contabilización:** La arquitectura debe soportar mecanismos que habiliten la auditoría de entidades simples y la aplicación subsiguiente cuando sea apropiado. Las redes de acceso deben proporcionar una forma segura, confiable y eficiente para colectar y gestionar datos de contabilidad para soportar diferentes eventos de negocio.
10. **Conocimiento de entorno:** Debe soportar una infraestructura común para el conocimiento del entorno a través de todas las funciones en el espacio de control del ambiente para adaptar la disponibilidad y entrega de servicios a redes heterogéneas en ambientes cambiantes dinámicamente.

2.2 Escenarios globales

Las redes móviles futuras proporcionarán a los usuarios móviles acceso a redes inalámbricas y móviles sin importar la tecnología o el dominio administrativo. Además, los servicios serán proporcionados de forma continua y sin interrupciones debidas a cambios de tecnologías de acceso o dominio administrativo. El protocolo IP será la base para ser ejecutado extremo a extremo entre dispositivos móviles, aplicaciones y servicios. Un escenario típico es mostrado en la figura 5.

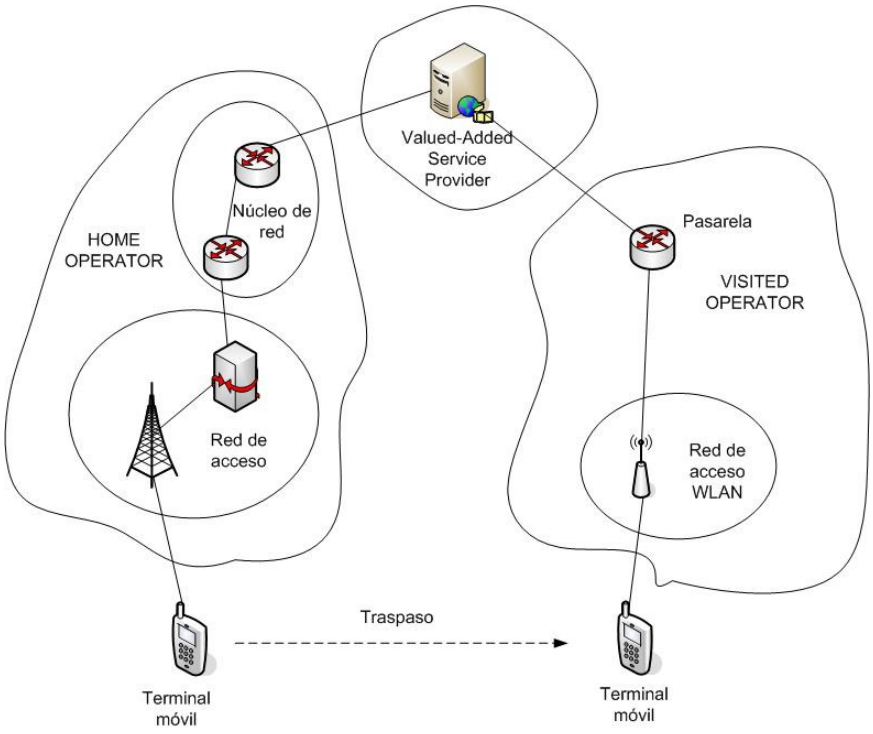


Figura 3.1 – Escenario global

En este escenario se asume que el usuario tiene una subscripción con un operador de red, conocido como "Home Operator" (HO). Este operador tiene una serie de acuerdos de roaming con otros operadores de red, los cuales son conocidos como "Visitor Operators" (VO), con lo cual, el usuario puede usar los recursos de esos operadores sin ningún problema. Por otro lado, existen otros participantes que proporcionan servicios que los operadores no pueden proporcionar, estos operadores son conocidos como proveedores de servicio de valor añadido (Value-Added Service Provider – VASP). Por lo tanto, el usuario será facturado tanto por el uso del servicio como por el uso de los recursos de red. Esto implica que se debe de realizar una medición por los dos conceptos descritos anteriormente.

Del escenario definido anteriormente se puede observar que existen un conjunto de entidades globales que participan en el proceso de prestación de servicios en un ambiente de redes móviles. A continuación se explica cada una de las entidades globales y el papel que desempeña cada una de ellas durante el proceso de prestación de servicios.

- ***"Home Operator" (HO)*** es el operador con el cual el usuario tiene una subscripción. Cuando el usuario se conecta a su HO, los mecanismos de tarificación son locales, lo cual representa el escenario más simple de tarificación.

- ***"Visitor Operator" (VO)*** es el operador que proporciona el servicio de conexión sin disponer de acuerdo directo con el usuario, aunque si que tiene acuerdos de roaming con el operador del usuario.

- ***"Value-Added Service Provider" (VASP)*** es el que proporciona cualquier servicio que no está incluido dentro de la red HO o VO, y que el usuario puede acceder vía la conexión a través de esas redes.

El HO es el que mantiene la información del perfil de usuario, el cual es requerido para el proceso de facturación final, el cual es elaborado por el HO. El VO es introducido como la entidad que permite al usuario llevar a cabo el proceso de roaming. Los detalles del servicio de roaming son proporcionados en el acuerdo de roaming entre HO y VO. Además existe una relación entre el VASP y el HO o VO, en la cual el HO o VO gestionan la relación entre usuario y VASP. En esta situación el operador móvil (HO o VO) entregan el contenido al usuario. Por otro lado, puede existir una relación directa con el usuario, en el caso de que el usuario tenga una suscripción directa con el VASP, en cuyo caso, el VASP desempeñará la tarificación y la facturación directamente al usuario.

Sin embargo, para un mejor análisis de las entidades que participan en el proceso de prestación de servicios en redes móviles, es necesario definir que también cada una de las entidades que prestan los servicios se rigen por un modelo de gestión, comúnmente denominado dominio de gestión y que los operadores de red pueden tener el control de diferentes tecnologías de acceso, con lo cual, el proceso de tarificación se complica aún más. Un dominio de gestión lo definiremos como la parte de la red del operador que se

encuentra administrada por un mismo modelo de gestión. Con esta referencia tendremos un ambiente en donde existirán diferentes proveedores de servicios, con diferentes modelos de gestión, así como una serie de operadores de red controlando diferentes tecnologías de acceso (UMTS, GSM, WiFi, etc.) lo cual involucra diferentes dominios de gestión. Con esto, se debe realizar un análisis de todos los posibles escenarios que se generarían de este nuevo entorno para la gestión de la tarificación, aunque previamente a ello, se propondrán más detalladamente las entidades que compondrán el HO, VO y VASP.

2.3 Entidades propuestas

Siguiendo los requerimientos generales y basándonos en los escenarios globales, la arquitectura de tarificación propuesta estará formada por las siguientes entidades individuales:

AA → Servidor de Autenticación y Autorización
CT → Contenedor de Información de Tarificación
ES → Elemento de Servicio
FGT → Función de Gestión de la Tarificación
FU → Ficha de Usuario
SM → Sonda de Medición

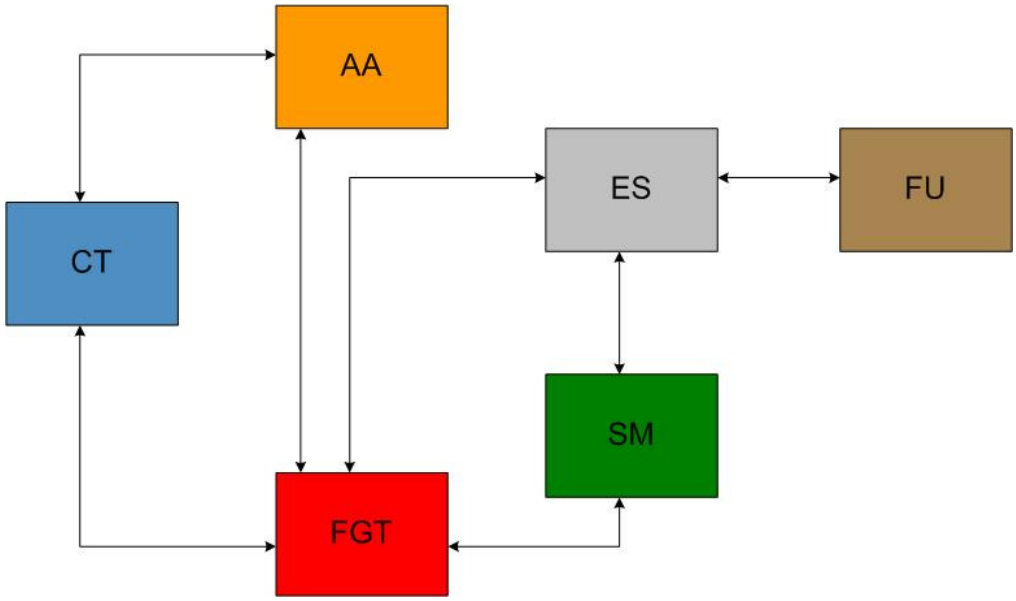


Figura 3.2 – Entidades de la arquitectura propuesta

2.3.1 CT (Contenedor de Información de Tarificación)

El repositorio de información es la entidad que almacena la información que es relevante para el proceso de tarificación. Esta entidad está a su vez compuesta por 4 repositorios:

User Profile → Es el repositorio donde se almacena toda la información relacionada al usuario como son los datos personales, datos para autenticación y autorización y el SLA contratado por el usuario

Accounting → Es el repositorio donde se almacenarán todos los registros de tarificación de los usuarios.

Policies → Es el repositorio donde se almacenan las diferentes políticas que serán aplicadas durante el proceso de tarificación a los usuarios basados en sus perfiles.

UCP → Es el repositorio donde se almacenará el registro de conexión del usuario.

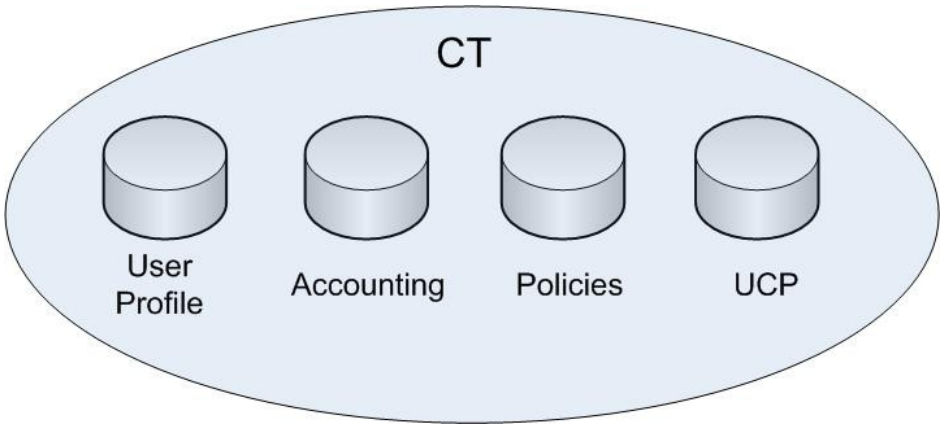


Figura 3.3 – Composición del Contenedor de Información de Tarificación

2.3.2 FGT (Función de Gestión de la Tarificación)

La FGT es la entidad del modelo que realiza el control de la tarificación mediante la gestión de políticas.

Esta entidad podrá desempeñar los siguientes papeles:

- ***Coordinador de tarificación*** → Realiza la coordinación de todo el proceso de tarificación relacionado con los servicios activos del usuario. Estará localizado en el dominio del HO.

- ***Proxy de tarificación*** → Realiza la gestión de control de crédito y control intermedio del proceso de tarificación para una serie de servicios activos del usuario dentro de una misma tecnología de red. Estará ubicado en la red de acceso del usuario.

- ***Tarificador remoto*** → Desempeñará la monitorización del uso de servicios de valor añadido por parte del usuario y reportará al proxy de tarificación los resultados del monitoreo, además actuará como intermediario en el proceso de petición de crédito para los servicios de valor añadido.

La entidad estará formada por los siguientes módulos:

- ***PDP (Policy Decision Point)*** → Este módulo será el responsable de la toma de decisiones sobre las políticas a ser aplicadas a cada usuario para el proceso de tarificación, basado en el perfil de usuario y el SLA dinámico contratado.

- ***PR (Policy Recipient)*** → Se encarga del procesamiento de los registros de uso de recursos y del almacenamiento para su uso en la facturación.

- ***CC (Charging Control)*** → Controla el crédito disponible mediante la asignación de crédito y la monitorización de los cargos relacionados al uso del servicio. Además reporta el uso de los recursos del usuario para el proceso de tarificación.

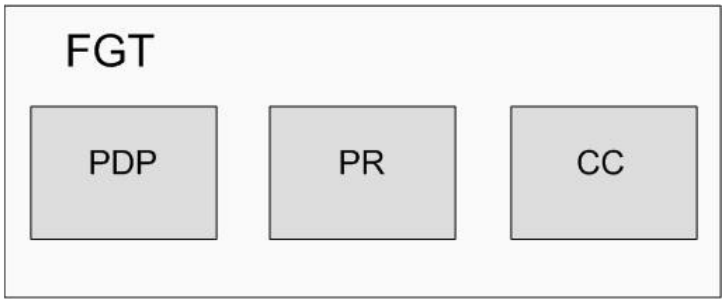


Figura 3.4 – Composición de la Función de Gestión de la Tarificación

2.3.3 AA (Autenticación y Autorización)

Es la entidad responsable de llevar a cabo el proceso de autenticación y autorización de los usuarios mediante una serie de políticas de control de acceso. Al ser la tarificación un proceso crítico, no en cuanto al tiempo de ejecución sino a la seguridad con la que este proceso se debe llevar a cabo, será necesario que en todo momento se tenga la certeza de que el terminal móvil y/o el usuario estén autorizados para el uso de los servicios. Para ello, en determinadas fases de las conexiones se llevarán a cabo autenticaciones de los terminales y/o usuarios. Por ejemplo, en el envío de la información de tarificación, de alguna manera el sistema debe asegurarse de que el terminal al que le está dando servicio no es ningún equipo no registrado que esté consumiendo recursos de forma ilegal. También se podría requerir una autenticación a la hora de cambiar de servicio, ya que el sistema se debería de asegurar de que el usuario y/o terminal tuvieran derechos para usar ese servicio.

Las autenticaciones pueden ser de dos tipos, de terminal y de usuario:

- ***Autenticación de terminal*** → Se realiza para verificar que el equipo que se utiliza para acceder a la red está registrado internacionalmente, que no es ningún equipo extraviado o extraído y que no accederá de modo ilegal a los servicios proporcionados por la red. Este tipo de autenticación se puede llevar a cabo mediante el uso del IMSI (International Mobile Subscriber Identity).

- ***Autenticación de usuario*** → Se realiza para verificar que el usuario que va a utilizar un determinado servicio está autorizado para ello, ya que existe un acuerdo previo entre el proveedor de servicios de valor añadido y el usuario que le permite acceder a ellos. Este tipo de autentificación se podría llevar a cabo mediante el uso de claves compartidas o certificados que previamente hubieran sido proporcionados por el proveedor de servicios.

2.3.4 SM (Sonda de Medición)

La sonda de medición es la entidad responsable de realizar la medición y la recopilación de los datos de uso de recursos por parte del usuario, es decir, una recopilación de paquetes que contengan datos específicos a los diferentes consumos que hayan realizado los usuarios, según los baremos establecidos por las distintas políticas de tarificación de que disponga el operador.

Se han definido dos tipos de sondas de medición:

- ***Sondas estáticas*** → En las cuáles todos los flujos son medidos de igual manera, bajo el mismo criterio global. En muchos casos la gran cantidad de datos capturados las hace necesarias.

- ***Sondas configurables*** → En las cuáles se colectan datos de medición siguiendo las pautas que marcan las políticas de medición para determinados flujos especificados.

2.3.5 FU (Ficha de Usuario)

Es la tarjeta de identificación del usuario, y la cual le permite hacer uso de los servicios dentro de la red. Esta ficha de usuario estará formada por:

- Un módulo de decisión de políticas de acceso
- Un repositorio de perfil de conexión de usuario (UCP)
- Un repositorio de políticas de preferencia de acceso
- Una copia del SLA contratado
- Una unidad de control de crédito

Además, también dispondrá de las distintas claves privadas y/o certificados necesarios para poder acceder a determinados servicios que tenga contratados.

2.3.6 ES (Elemento de Servicio)

Es la entidad funcional que proporciona un servicio final al usuario. Ejemplos de servicios finales podrían ser: Servidor de Acceso a la Red (NAS – Network Access Server), Servidor Proxy SIP (Session Initiation Protocol), servidores de aplicaciones, etc.

3 Escenarios de traspaso

3.1 Visión general

En una red de comunicaciones móviles avanzada las diferentes tecnologías pueden operar en ambientes públicos, corporativos y residenciales. Estos ambientes dan lugar a una gran variedad de escenarios en donde se pueden involucrar diferentes dominios administrativos y diferentes grados de integración de red.

- Un operador es propietario de varias tecnologías de acceso.
- Operadores individuales de tecnologías de acceso radio.
- Los operadores tienen un acuerdo de cooperación completo.
- Los operadores tienen un acuerdo parcial de colaboración.
- Los operadores no tienen ningún acuerdo de colaboración.

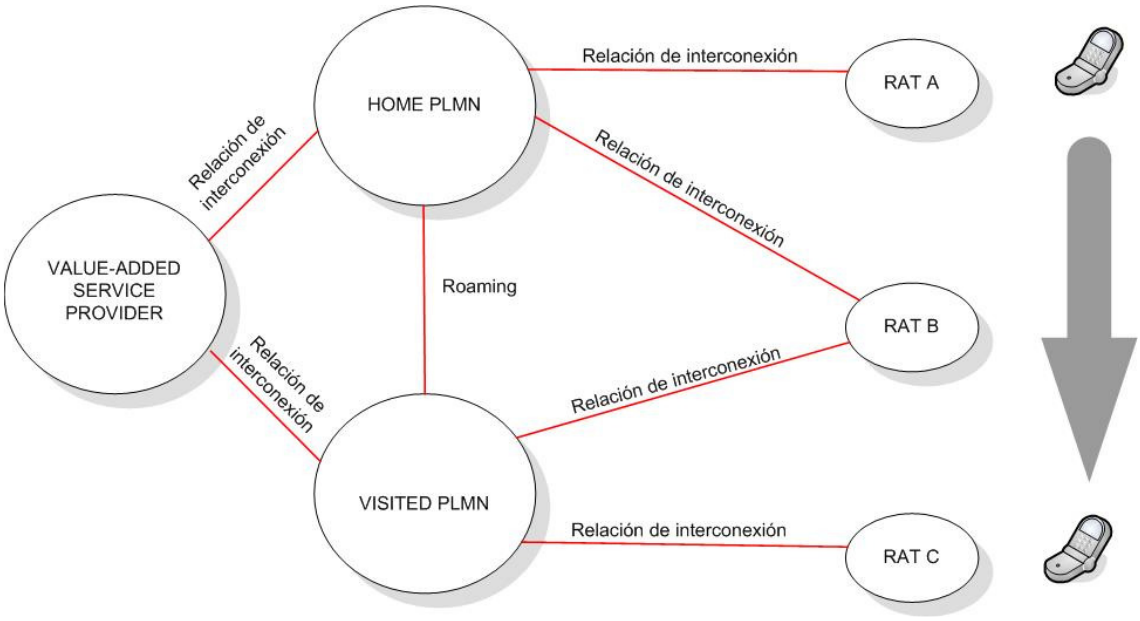


Figura 4.1 – Esquema del escenario global

Basado en las consideraciones mencionadas anteriormente, se pueden definir los siguientes escenarios.

3.1.1 Escenario 1 (Traspaso de dominio, mismo VASP)

Este primer escenario define el traspaso de dominio de gestión a nivel de VASP. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen al mismo VASP. Este escenario involucra dos situaciones, que el

usuario esté conectado al HO o que el usuario esté conectado al VO. En cualquiera de los casos el traspaso es realizado solamente a nivel de VASP, con lo cual el intercambio de información de contexto es realizado entre dominios de gestión que pertenecen al mismo VASP. La figura 4.2 muestra un ejemplo del Escenario 1.

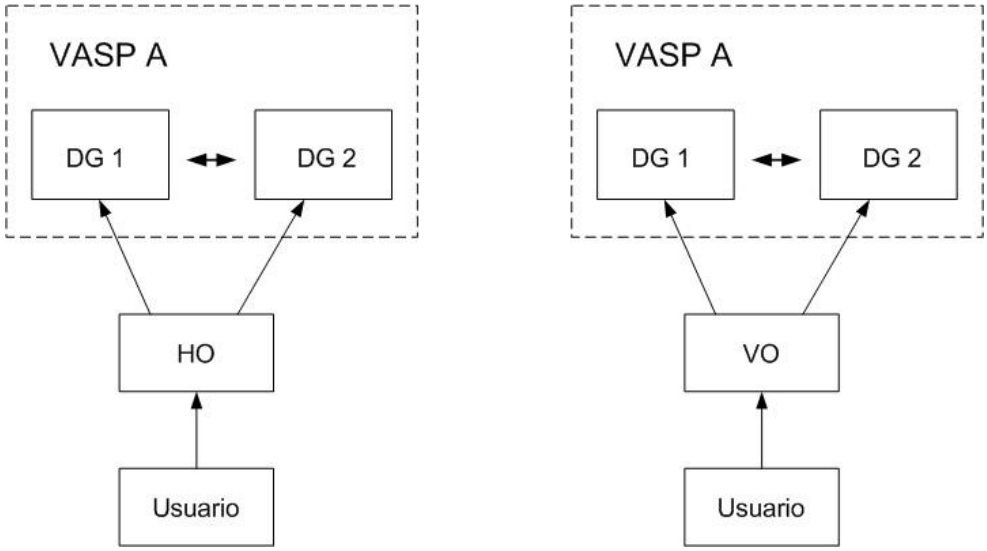


Figura 4.2 – Ejemplo del Escenario 1

3.1.2 Escenario 2 (Traspaso de dominio, diferente VASP)

Este escenario define el traspaso de dominio de gestión a nivel de VASP. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen a diferente VASP. Este escenario involucra dos situaciones, que el usuario esté conectado al HO o que el usuario esté conectado al VO. En cualquiera de los dos casos el traspaso es realizado solamente a nivel del VASP, con lo cual el intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes VASP. La figura 4.3 muestra un ejemplo del Escenario 2.

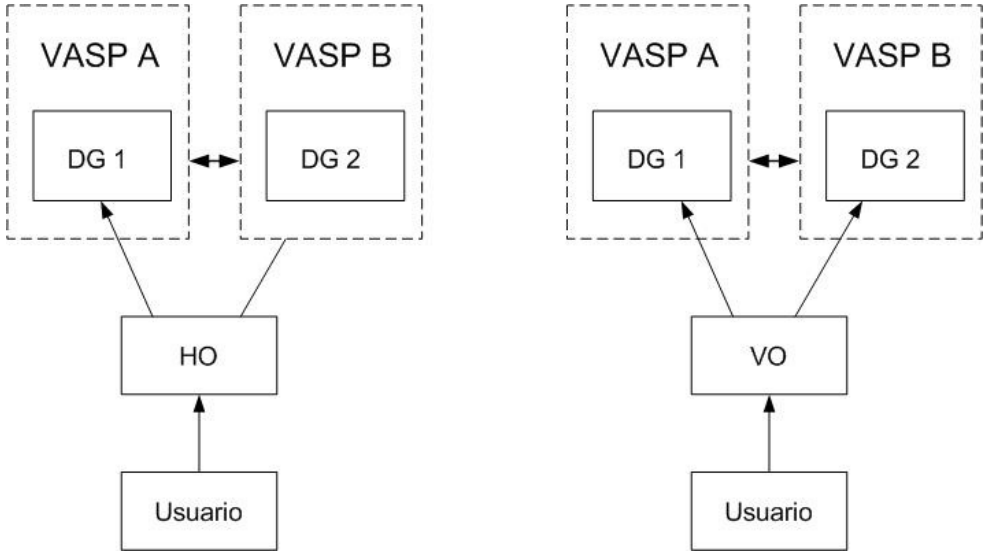


Figura 4.3 – Ejemplo del Escenario 2

3.1.3 Escenario 3 (Traspaso de dominio, diferente VASP, no acuerdo directo)

Este escenario define el traspaso de dominio de gestión de VASP. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen a diferente VASP con los que el usuario no tiene acuerdo directo. Este escenario involucra dos situaciones, que el usuario esté conectado al HO o que el usuario esté conectado al VO. En cualquiera de los casos el traspaso es realizado solamente a nivel de VASP, con lo cual el intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes VASP. La figura 4.4 muestra un ejemplo del Escenario 3.

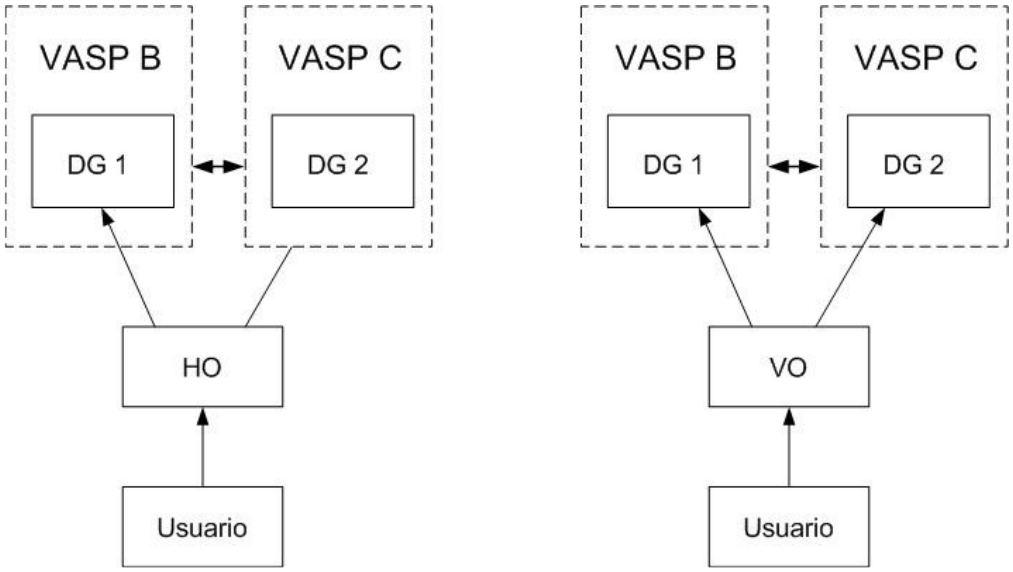


Figura 4.4 – Ejemplo del Escenario 3

3.1.4 Escenario 4 (Traspaso de dominio, mismo operador de red, misma RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen al mismo operador de red. Este escenario involucra dos situaciones, que el usuario esté conectado al HO o que el usuario esté conectado al VO. En cualquiera de los casos el traspaso es realizado solamente a nivel de operador de red, con lo cual el intercambio de información de contexto es realizado entre dominios de gestión que pertenecen al mismo operador de red. La figura 4.5 muestra un ejemplo del Escenario 4.

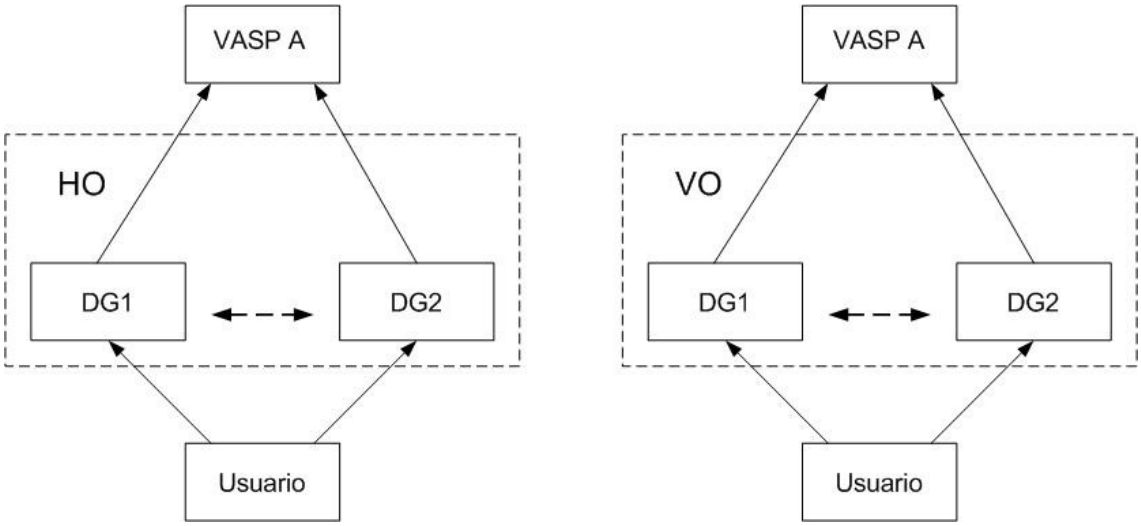


Figura 4.5 – Ejemplo del Escenario 4

3.1.5 Escenario 5 (Traspaso de dominio, mismo operador, diferente RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen al mismo operador. Este escenario involucra dos situaciones, que el usuario esté conectado al HO o que el usuario esté conectado al VO. El punto relevante es el hecho que se haga un traspaso a otra RAT que es controlada por el mismo operador. En cualquiera de los casos el traspaso es realizado solamente a nivel de operador de red, con lo cual el intercambio de información de contexto es realizado

entre dominios de gestión que pertenecen al mismo operador de red. La figura 4.6 muestra un ejemplo del Escenario 5.

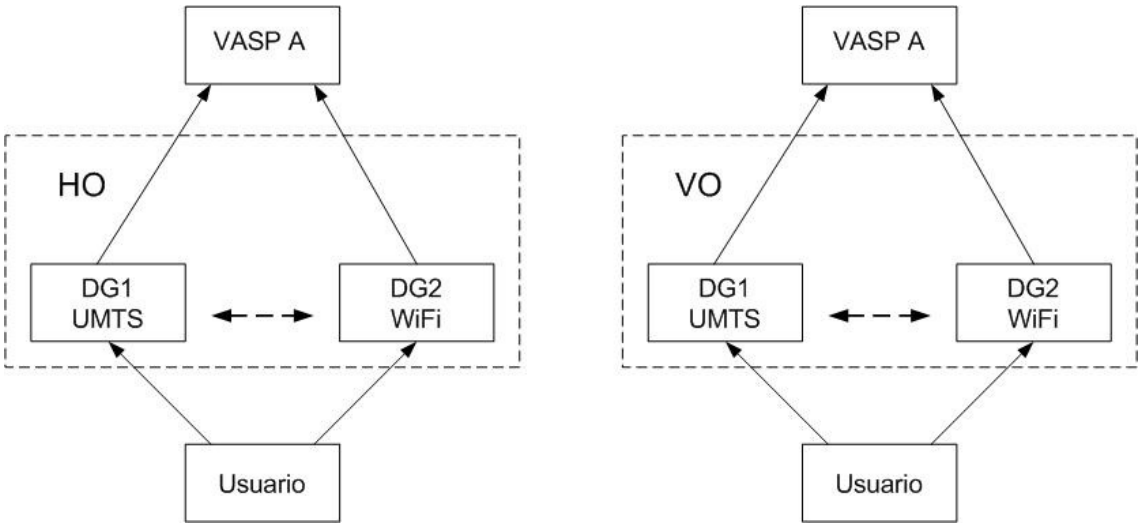


Figura 4.6 – Ejemplo del Escenario 5

3.1.6 Escenario 6 (Traspaso de dominio, diferente operador, misma RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso de usuario de un dominio de gestión a otro, uno de los cuales pertenece al HO y el otro al VO. Este escenario involucra dos situaciones, que el usuario esté conectado al HO y traspase al VO o viceversa. En este escenario se considera que el traspaso es realizado dentro de la misma tecnología de acceso a la red (UMTS → UMTS, WiFi → WiFi). El intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes operadores de red. La figura 4.7 muestra un ejemplo del Escenario 6.

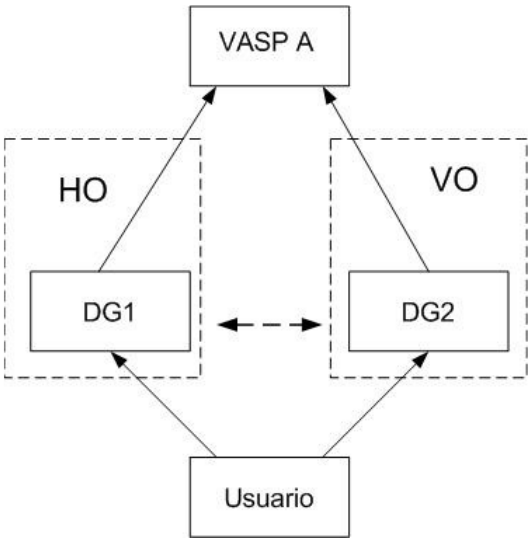


Figura 4.7 – Ejemplo del Escenario 6

3.1.7 Escenario 7 (Traspaso de dominio, diferente operador, diferente RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, uno de los cuales pertenece al HO y el otro al VO. Este escenario involucra dos situaciones, que el usuario esté conectado al HO y realice un traspaso al VO o viceversa. Un punto importante a considerar en este escenario es el hecho que el traspaso se realice hacia tecnologías de acceso a red diferentes (UMTS → WiFi, WiFi → UMTS). El intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes operadores de red. La figura 4.8 muestra un ejemplo del Escenario 7.

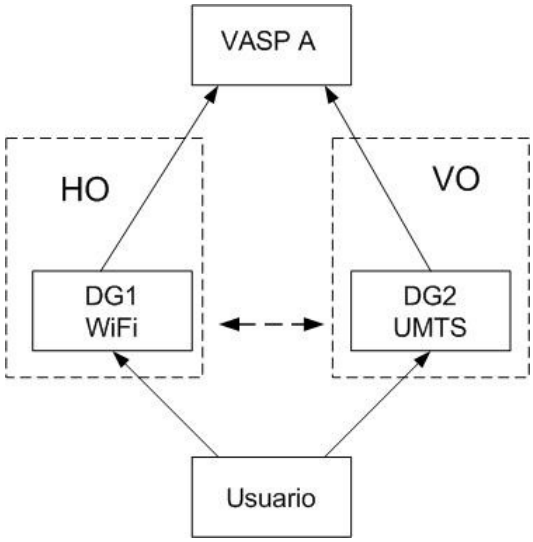


Figura 4.8 – Ejemplo del Escenario 7

3.1.8 Escenario 8 (Traspaso de dominio, diferente operador, misma RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen a diferentes operadores con los que el usuario no tiene acuerdo directo. Se considera que el traspaso es realizado dentro de una misma tecnología de red (UMTS→UMTS, WiFi→WiFi). El intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes operadores de red. La figura 4.9 muestra un ejemplo del Escenario 8.

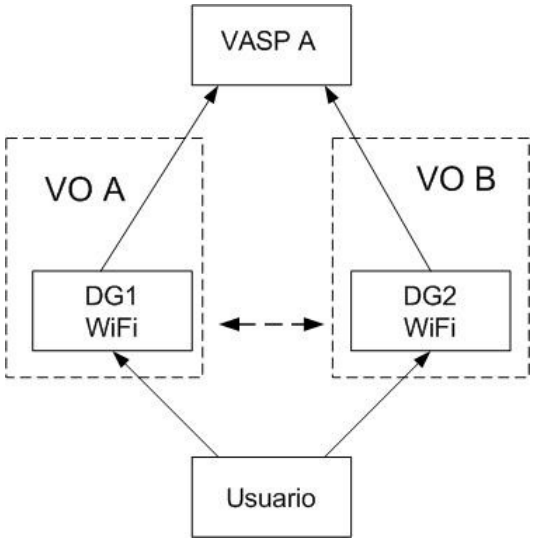


Figura 4.9 – Ejemplo del Escenario 8

3.1.9 Escenario 9 (Traspaso de dominio, diferente operador, diferente RAT)

Este escenario define el traspaso de dominio de gestión a nivel de operador de red. En este caso lo que se especifica es el traspaso del usuario de un dominio de gestión a otro, los cuales pertenecen a diferente operador y el usuario no tiene un acuerdo directo con ninguno de ellos. Se considera que el traspaso es realizado dentro de diferentes tecnologías de red (UMTS→WiFi, WiFi→UMTS). El intercambio de información de contexto es realizado entre dominios de gestión que pertenecen a diferentes operadores. La figura 4.10 muestra un ejemplo del Escenario 9.

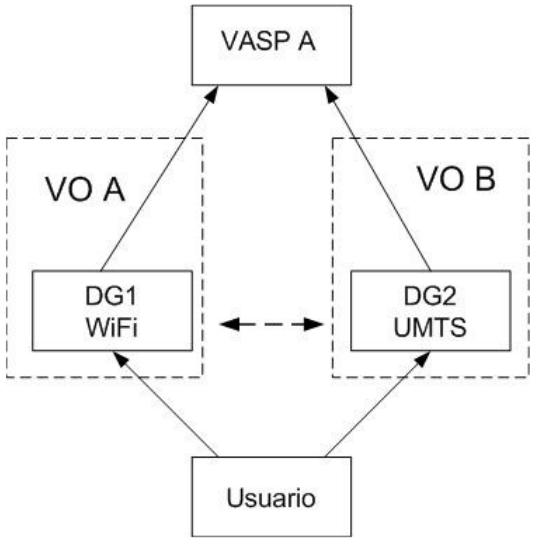


Figura 4.10 – Ejemplo del Escenario 9

3.2 Escenario de simulación

Para evaluar el rendimiento de la arquitectura diseñada dentro del ambiente de comunicaciones móviles avanzado nos basaremos en el siguiente escenario de simulación mostrado en la figura 4.11.

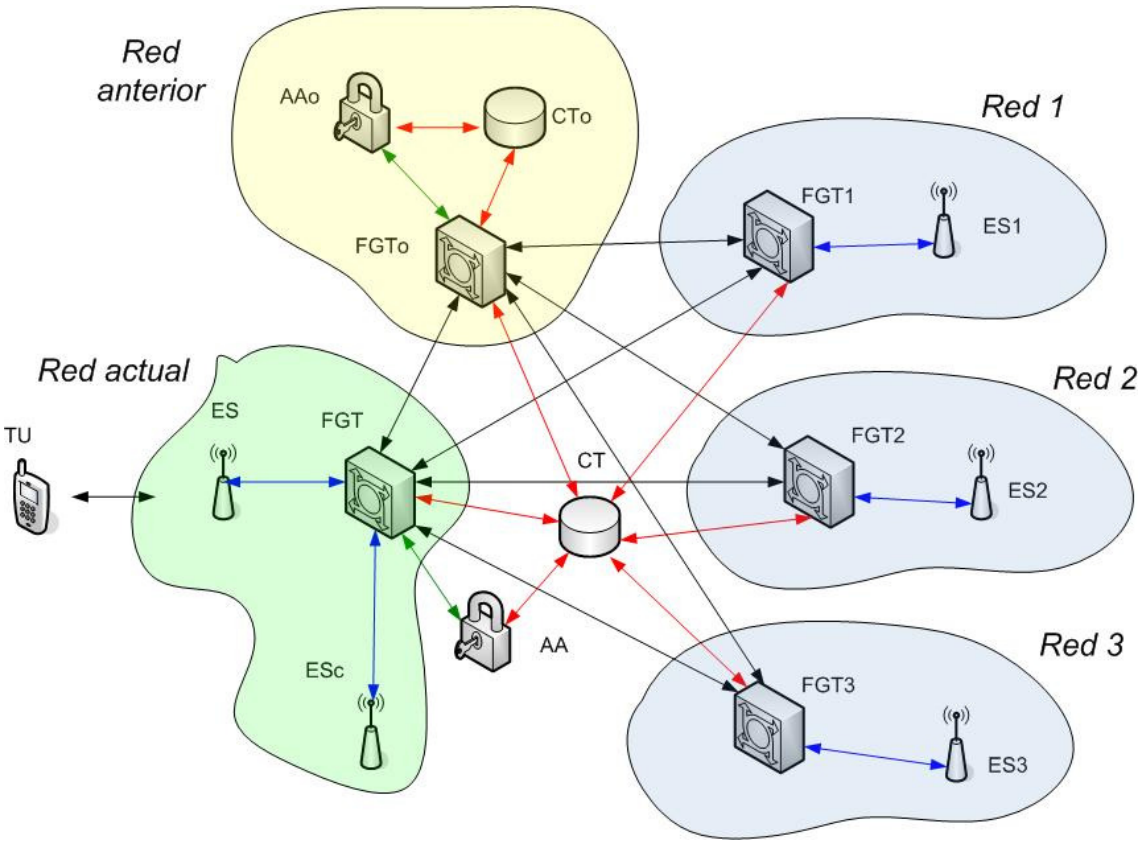


Figura 4.11 – Esquema del escenario de simulación

Dentro de este escenario tenemos una topología de 5 celdas de acceso. La celda que atiende las peticiones realizadas por los usuarios es la celda ES, y en la simulación es representada por una celda UMTS. Los usuarios pueden realizar dos tipos de peticiones: peticiones de traspaso y peticiones de nuevo servicio. Las peticiones de traspaso de los usuarios provendrán de la celda FGTo, que corresponderá a la última red en la que estuvo conectado el usuario. A parte de estas dos celdas mencionadas, también se dispone de 3 celdas más pertenecientes a distintos operadores y/o dominios de gestión a las que también se les podrán asignar las diferentes peticiones de los usuarios.

La topología es flexible a cualquier tipo de configuración en cuanto a operadores y dominios de gestión se refiere, es decir, cada red de las que se encuentra en el esquema podría pertenecer a cualquier operador y/o dominio de gestión diferente sin que el flujo de mensajes de señalización varíe significativamente. Los factores que harán variar levemente la señalización entre entidades serán: el operador de la nueva red (si es o no el HO), la celda escogida, el tipo de petición (si es de nuevo servicio o de traspaso) y el tipo de autentificación que se lleva a cabo (si es en serie o en paralelo).

Procesos como el traspaso serán tenidos en cuenta en la tarificación cuando éstos impliquen un cambio en la tarifa a aplicar a los servicios recibidos. Algunas de las razones por las que los traspasos podrían ser tenidos en cuenta en la tarificación serían los cambios de dominios de gestión, los cambios de red, el uso de nuevos servicios, el uso de diferentes tecnologías de transmisión, etc.

En referencia al proceso de autentificación, éste afecta al protocolo en varios aspectos. El principal aspecto a tener en cuenta es el retardo que introduce la autentificación en la señalización del proceso de traspaso. Este retardo extra hace que el traspaso no se pueda dar por válido hasta que la autentificación del terminal y/o el usuario se hayan realizado de forma satisfactoria. Por lo tanto, para reducir el retardo global del traspaso se debe reducir al máximo la repercusión de la autentificación en la señalización que se lleva a cabo, para ello, tal y como se verá más adelante, se han analizado dos procesos diferentes de autentificación, la autentificación en paralelo y la autentificación en serie. Otro aspecto a tener en cuenta sobre la autentificación sería estudiar las consecuencias de una autentificación errónea en el devenir del protocolo, aunque este aspecto no se considera en las simulaciones realizadas. En las simulaciones se presupone que las autentificaciones se llevan a cabo de forma satisfactoria y que los terminales y usuarios son validados sin ningún problema.

El caso estudiado dispone de 3 celdas UMTS y 2 celdas GSM, las cuáles, tal y como hemos mencionado anteriormente, pueden pertenecer a cualquier operador y/o dominio de gestión. Las peticiones, ya sean de nuevo servicio o de traspaso, son generadas mediante un tráfico a ráfagas con una tasa de llegadas que oscila entre las 10 y las 100 peticiones por ráfaga.

Características de las ráfagas	
Tiempo entre ráfagas	5 s – Distribución exponencial
Tiempo entre peticiones de una misma ráfaga	0,1 s – Distribución exponencial

Serán ofrecidos 2 tipos de servicios: voz y datos. Si la solicitud de servicio es asignada con éxito, los servicios de datos permanecerán en el sistema un tiempo de entre 6 – 8 segundos distribuidos uniformemente, y los servicios de voz entre 120 – 150 segundos también distribuidos de manera uniforme. Cada servicio tiene sus requerimientos de QoS , los cuales se detallan a continuación:

Tipo de servicio	**Requerimientos**
Voz	**BW** → 4 -25 Kbps
Datos	**BW** → 32 – 150 Kbps

Las celdas utilizadas para proporcionar el servicio están limitadas en capacidad, según si son celdas GSM o UMTS y además tienen sus propios retardos de servicio, los cuáles aumentan según la ocupación de la celda. Todos estos parámetros son utilizados por la FGT (Función de gestión de la Tarificación) para que mediante un algoritmo de selección de celda [10] se escoja la que mejor servicio podrá proporcionar al usuario.

3.3 Flujo de señalización

El camino que llevan a cabo las distintas peticiones generadas por los usuarios se rige por el siguiente patrón:

1 – La petición, ya sea, de nuevo servicio o de traspaso llega al ES y éste la reenvía después de procesarla hacia la FGT.

2 – Una vez llegada la petición a la FGT, ésta solicita al CT la información referente a los recursos disponibles en las distintas redes a las que tiene conexión.

3 – Una vez la FGT ha recopilado la información referente a los recursos disponibles en las distintas redes colindantes, ejecuta el algoritmo de selección de celda para escoger la celda mejor capacitada para dar el servicio solicitado.

4 – Una vez escogida la celda que proporcionará el servicio, según el tipo de autentificación programado se seguirá un procedimiento u otro:

> → ***AA Serie*** *(*):* Se solicita la autentificación del usuario que ha generado la petición y dependiendo de si la red escogida pertenece o no al HO se realizará un procedimiento u otro:
>
> ***1*** **–** Si la nueva celda escogida pertenece al HO: La autentificación se realizará con el servidor AA perteneciente a la red del HO.
>
> ***2*** **–** Si la nueva celda escogida no es propiedad del HO: la autentificación se realizará mediante consulta a la última red a la que ha estado conectado el usuario. De esta manera se consigue reducir el retardo respecto a una autentificación con el HO, que podría ubicarse en cualquier lugar del mundo, con su consiguiente repercusión en el retardo general del proceso.
>
> Una vez autentificado el usuario, se pasarán a configurar los dispositivos implicados en prestar el servicio a la petición recibida.
>
> → ***AA Paralelo*** *(*)*: Se realiza de forma paralela la solicitud de autentificación del usuario que ha generado la petición y la configuración de los dispositivos implicados en prestar el servicio a la petición. Cada procedimiento se va ejecutando de forma independiente al otro. En el caso de la autentificación, si ésta resultase errónea, ya se encargarían otros mecanismos de nivel más alto de rechazar al usuario que había entrado al sistema. Este tipo de autentificación puede provocar que haya un intervalo de tiempo en el que cualquier usuario pueda disfrutar de algún servicio sin tener realmente privilegios para ello, aunque este intervalo de tiempo sería insignificante. Además, el hecho de que un usuario esté ya dentro de la red, significa que hay un mínimo de confianza entre el usuario y el operador como para permitirse este pequeño *"agujero"* de seguridad.

(*) **NOTA:** Se presupone que en los procesos de autentificación el usuario envía hacia la FGT una petición de traspaso o de nuevo servicio y en el mensaje adjunta su IMSI o cualquier

otro dato que lo identifique a él o al terminal, como podría ser algún tipo de clave o el uso de algún certificado, para poder llevar a cabo el traspaso o acceder al nuevo servicio. La FGT envía el dato identificativo del usuario o terminal hacia el servidor de AA, el cuál con los datos recibidos verificará que el usuario o terminal tienen los permisos necesarios para acceder a los nuevos servicios solicitados o para ejecutar el traspaso. Esta verificación la realizará o bien por simple comparación de los datos recibidos con los que tiene almacenados en el CT en el caso más simple, o bien mediante algoritmos de autentificación en los cuales se utilizan claves de diferentes tamaños o certificados en el caso más complejo. Al no ser el punto principal del estudio, no se profundizará en los tipos de algoritmos de autentificación usados ni en los tamaños y tipos de claves, certificados o datos identificativos de los usuarios o terminales.

3 – El Esn elegido para proporcionar el servicio actualiza la información del CT referente a la ocupación de su celda.

De forma esquemática se mostrarán a continuación los distintos flujos de señalización comentados anteriormente. Estos flujos de señalización se han dividido en 7 apartados diferentes, el primero (1) corresponde al proceso inicial que siguen todas las peticiones antes de ejecutar el algoritmo de selección de celda, los dos apartados siguientes (2-3) corresponden a la señalización de los procesos de autentificación cuando (2) la nueva celda escogida pertenece al HO y (3) cuando la nueva celda escogida no pertenece al HO. Finalmente, los últimos cuatro apartados (4-7) hacen referencia a la señalización utilizada para empezar a prestar el servicio solicitado por la petición recibida. La prestación del servicio se divide en los casos (4) Esn escogida para cursar un nuevo servicio, (5) Esn escogida para cursar un traspaso, (6) Esc escogida para cursar un nuevo servicio y (7) Esc escogida para cursar un traspaso

3.3.1 Proceso previo a la selección de celda

Cuando el sistema recibe una petición, ya sea de traspaso o de nuevo servicio, ésta es procesada por la FGT, la cual inmediatamente solicita al CT información acerca de la ocupación de recursos que tienen las redes colindantes. Posteriormente a la recolección de la información, mediante el algoritmo de selección de celda se elige la mejor red para cursar la petición recibida.

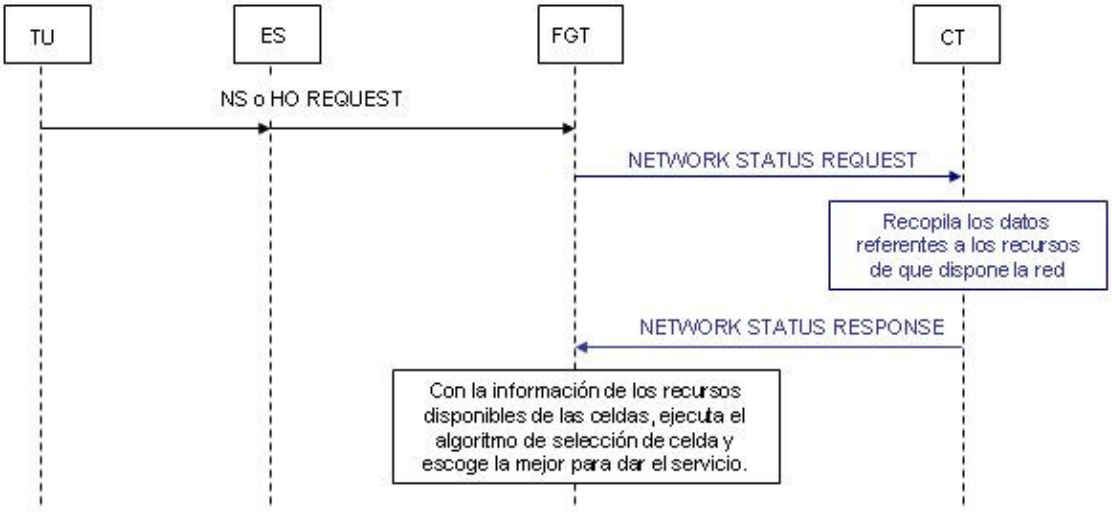


Figura 4.12 – Señalización del proceso previo a la selección de celda

3.3.2 Proceso de AA cuando la nueva celda escogida pertenece al HO

Después de haber escogido la celda más adecuada para cursar el servicio, si ésta pertenece a una red del HO, entonces la autentificación se realizará directamente contra el servidor de AA del mismo HO. El procedimiento será el siguiente: la FGT envía una petición de autentificación al servidor de AA, éste solicita al CT la información necesaria del usuario para corroborar que éste es quien dice ser y tiene los privilegios necesarios para acceder a los servicios que solicita. Una vez el servidor de AA tiene los datos necesarios para comprobar la identidad y los permisos del usuario, ejecuta el proceso necesario para hacer la comprobación. Cuando acaba el proceso de autentificación del usuario, se le indica a la FGT el resultado.

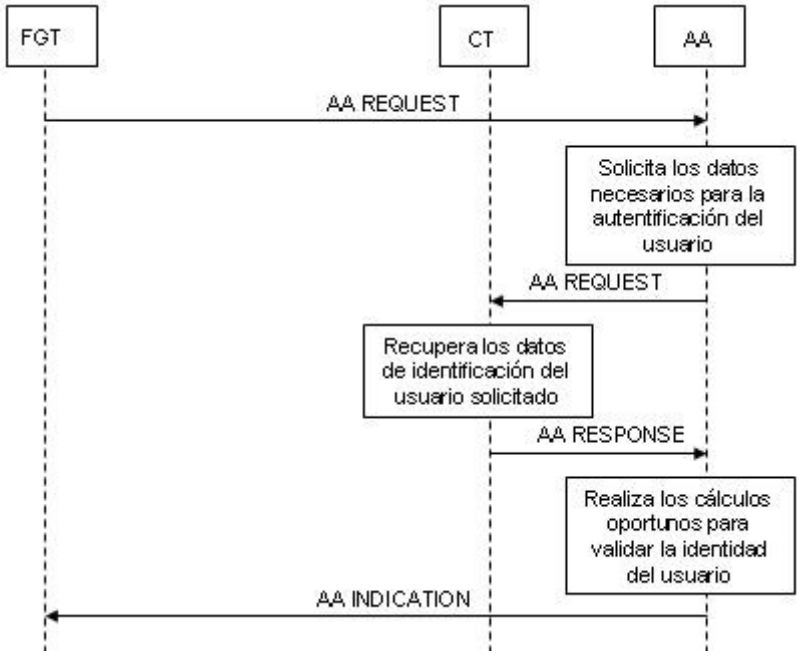


Figura 4.13 – Señalización del proceso de AA cuando la nueva celda escogida pertenece al HO

NOTA: Esta señalización es independiente de si se realiza la autentificación en serie o en paralelo. La diferencia entre hacer la autentificación en serie o en paralelo radica en que en la primera (serie), será necesaria una correcta autentificación del usuario previa a empezar a cursar los servicios solicitados y en la segunda (paralelo), se empezará a cursar el servicio sin todavía saber el resultado de la autentificación. En caso de que el usuario no cumpla los requisitos para percibir los servicios solicitados, otros procedimientos aquí no contemplados se encargarán de gestionar la expulsión del usuario de la red.

3.3.3 Proceso de AA cuando la nueva celda escogida NO pertenece al HO

En este caso, cuando la celda escogida más adecuada para prestar el servicio no pertenece a la red del HO, se actuará de otra manera para autentificar al usuario. Para obtener la mejor relación entre seguridad y retardo, se procederá de la siguiente manera: la FGT enviará una petición de autentificación a la FGTo (FGT de la última red en la que estuvo conectado y autenticado el usuario), y ésta procederá de la misma manera que en el caso anterior, es decir, enviará una petición de autentificación a su servidor de AA local (Aao), éste solicitará a su CT local (Cto) la información necesaria del usuario para corroborar que éste es quien dice ser y tiene los privilegios necesarios para acceder a los servicios que solicita. Y una vez el servidor de AA local (Aao) tiene los datos necesarios para comprobar la identidad y los permisos del usuario, ejecuta el proceso necesario para hacer la comprobación. Cuando acaba el proceso de autentificación del usuario, se le indica a la FGTo el resultado, y ésta informa finalmente a la FGT.

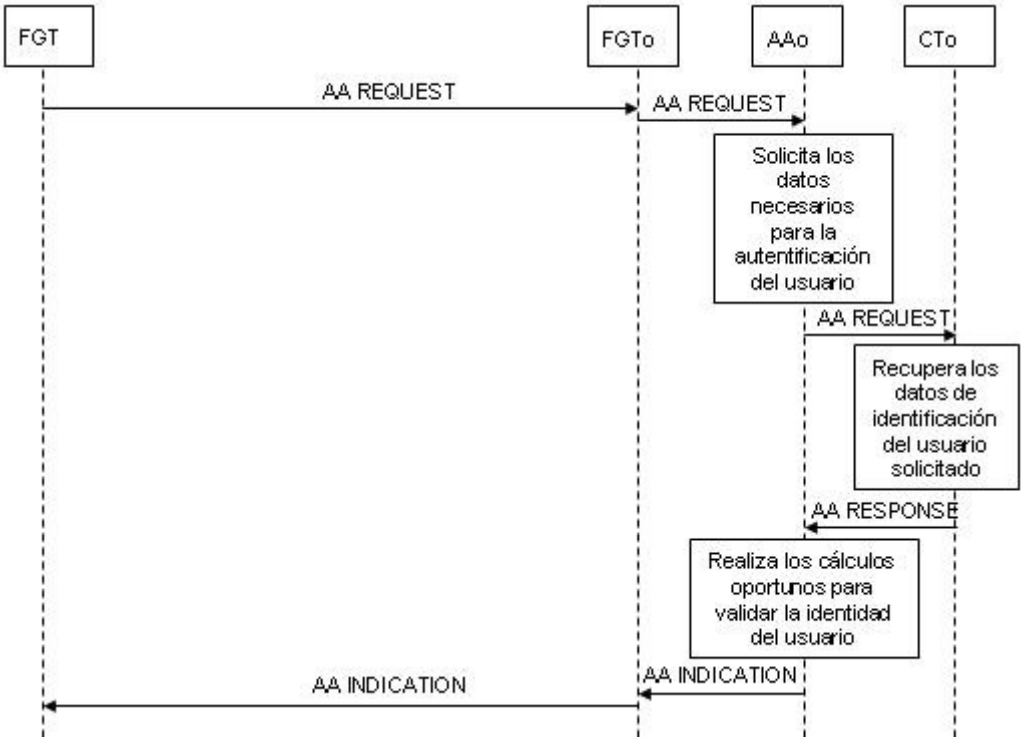


Figura 4.14 – Señalización del proceso de AA cuando la nueva celda escogida NO pertenece al HO

NOTA 1: En este tipo de autentificación también se aplica lo comentado en la nota del anterior caso de señalización respecto a las variantes de AA en serie y en paralelo.

NOTA 2: Se ha decidido utilizar la información de autentificación contenida en la última red a la que se estuvo conectado ya que se ha considerado la mejor manera de proporcionar un nivel razonable de seguridad manteniendo el retardo en niveles bajos respecto a lo que supondría tener que autentificarse con el HO que podría encontrarse a distancias mayores. En el caso de peticiones de traspaso esto es del todo correcto, pero en el caso de las peticiones de nuevo servicio no es lo más común, ya que la conexión no proviene de ningún sitio, sino que se ha generado desde cero, aunque por cuestiones de simplicidad se ha considerado que también podrían recuperar información de autentificación de una supuesta *"red anterior"*, utilizando el mismo modelo que en el caso de una petición de traspaso.

A continuación, para los casos (4-7) partiremos de la premisa que una vez se ha realizado la autentificación (caso AA en serie) o directamente cuando se ha recibido una petición y se ha escogido una celda para servirla (caso AA en paralelo) se empezará a enviar la señalización necesaria para cursar la petición recibida, señalización que dependerá del Esx escogido para dar el servicio y del tipo de petición a cursar.

3.3.4 Esn escogida para cursar una petición de nuevo servicio

En el caso de que la red escogida no sea la que actualmente está conectado el usuario y la petición solicitada sea un nuevo servicio, se procederá de la siguiente manera: se envía una petición de nuevo servicio a la FGT de la red escogida (FGTn). Una vez procesado el mensaje por la FGTn, ésta envía los parámetros de configuración del servicio a la celda correspondiente y notifica a la FGT de que el nuevo servicio ya se está cursando. Finalmente, la FGT informará de ello al TU (Terminal de usuario).

Mientras tanto, el Esn comienza a servir la petición y genera un nuevo mensaje con la actual ocupación de los recursos que será enviado a través de la FGTn hacia el CT, el cuál actualizará su información en referencia a la ocupación de las redes que controla.

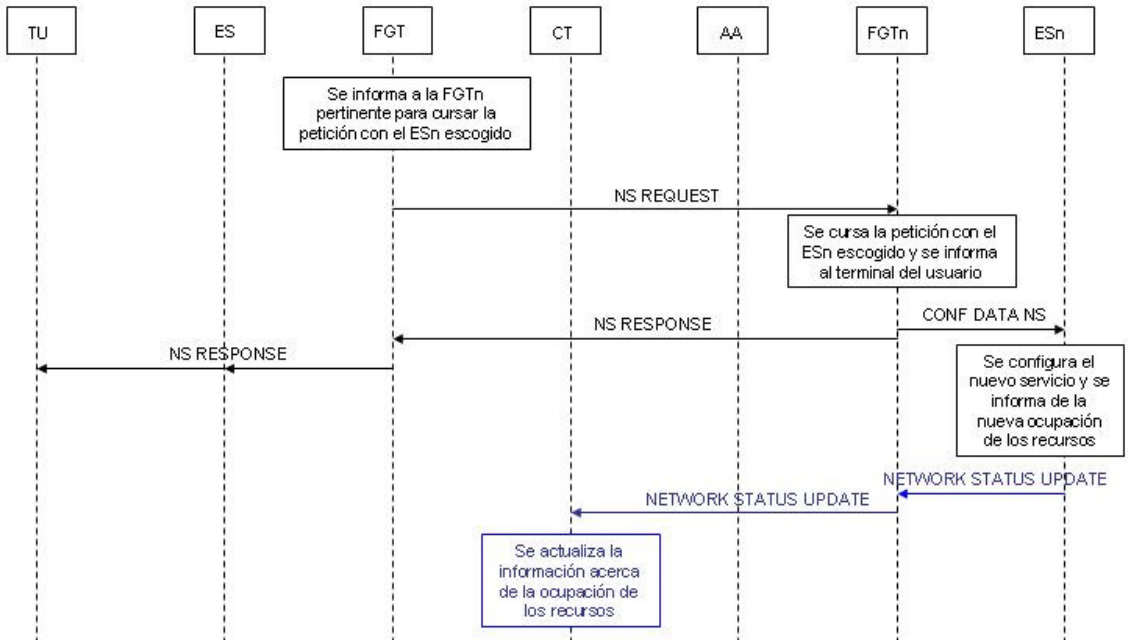


Figura 4.15 – Señalización cuando se escoge Esn para cursar una petición de nuevo servicio

3.3.5 Esn escogida para cursar una petición de traspaso

Si la red escogida no es la que actualmente está conectado el usuario y la petición solicitada es un traspaso, se procederá de la siguiente manera: se envía una petición de nuevo servicio a la FGT de la red escogida (FGTn). Una vez procesado el mensaje por la FGTn, ésta solicita los datos referentes a la configuración de los parámetros de tarificación a la FGT de la última red a la que estuvo conectado el usuario (FGTo). Una vez recibidos estos datos, la FGTn envía los parámetros de configuración del servicio a la celda correspondiente y notifica a la FGT de que el traspaso ya se está cursando. Finalmente, la FGT informará de ello al TU. Mientras tanto, el Esn comienza a servir la petición y genera un nuevo mensaje con la actual ocupación de los recursos que será enviado a través de la FGTn hacia el CT, el cuál actualizará su información en referencia a la ocupación de las redes que controla.

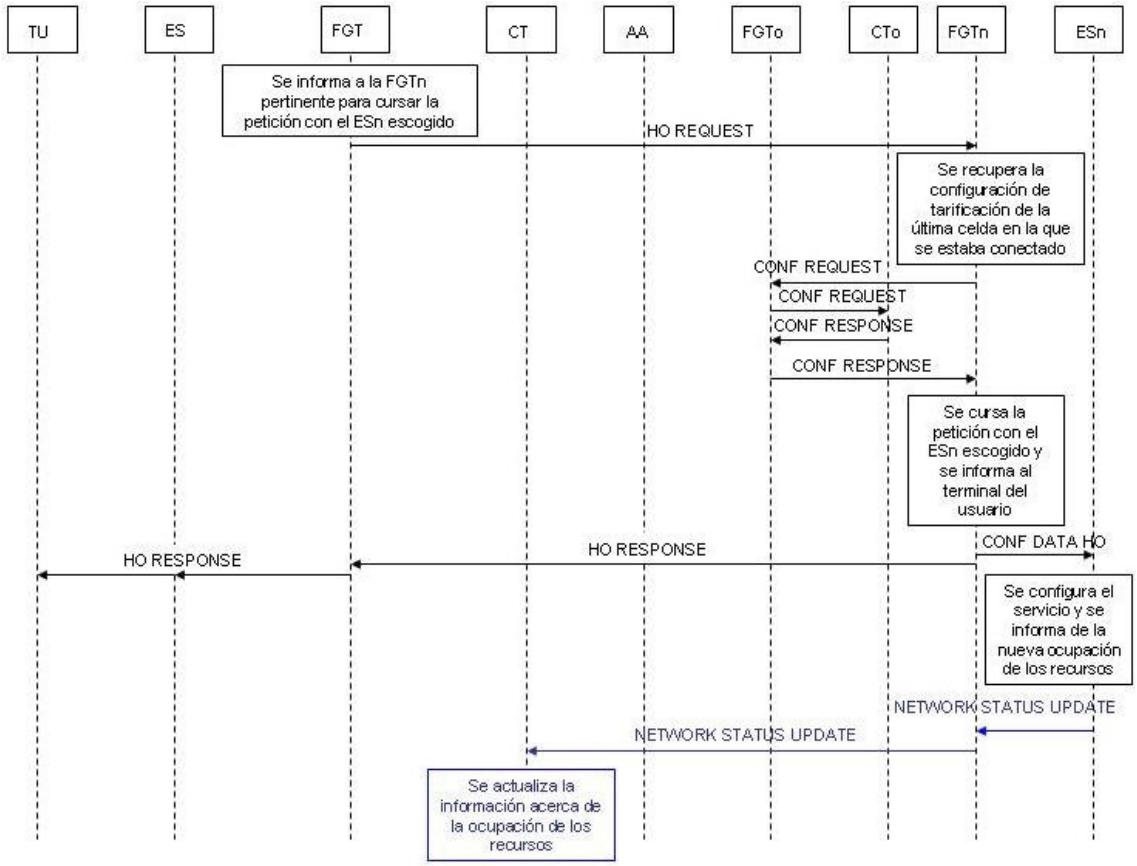


Figura 4.16 – Señalización cuando se escoge Esn para cursar una petición de traspaso

3.3.6 Esc escogida para cursar una petición de nuevo servicio

En el caso de que la red escogida sea la que actualmente está conectado el usuario y la petición solicitada sea un nuevo servicio, se procederá de la siguiente manera: con todos los datos de configuración recopilados, la FGT envía los parámetros de configuración del servicio a la celda correspondiente y notifica al TU de que el nuevo servicio ya se está cursando. Mientras tanto, el Esc comienza a servir la petición y genera un nuevo mensaje con la actual ocupación de los recursos que será enviado a través de la FGT hacia el CT, el cuál actualizará su información en referencia a la ocupación de las redes que controla.

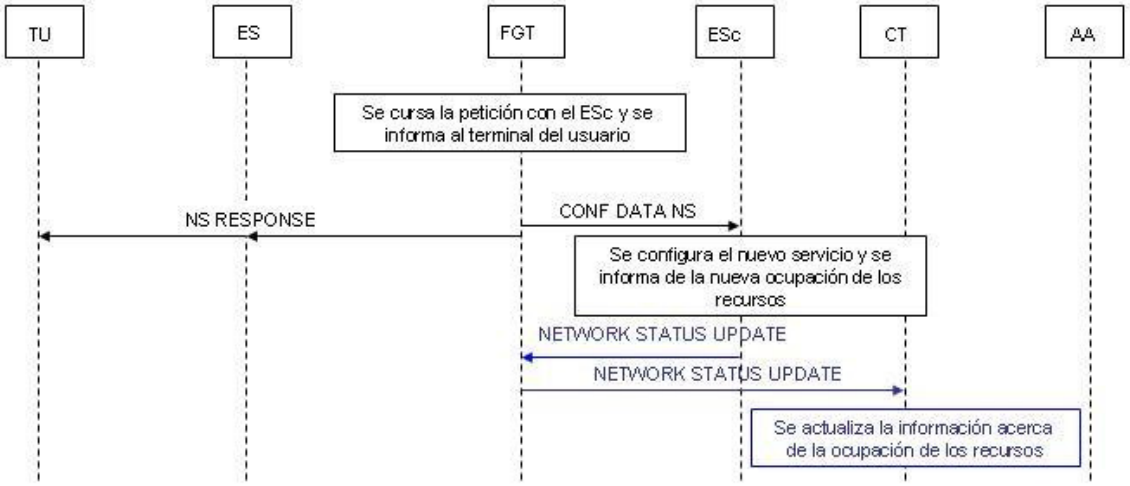


Figura 4.17 – Señalización cuando se escoge Esc para cursar una petición de nuevo servicio

3.3.7 Esc escogida para cursar una petición de traspaso

Si la red escogida es la que actualmente está conectado el usuario y la petición solicitada es un traspaso, se procederá de la siguiente manera: la FGT solicita los datos referentes a la configuración de los parámetros de tarificación a la FGT de la última red a la que estuvo conectado el usuario (FGTo). Una vez recibidos estos datos, la FGT envía los parámetros de configuración del servicio a la celda correspondiente y notifica al TU de que el traspaso ya se está cursando. Mientras tanto, el Esc comienza a servir la petición y genera un nuevo mensaje con la actual ocupación de los recursos que será

enviado a través de la FGT hacia el CT, el cuál actualizará su información en referencia a la ocupación de las redes que controla.

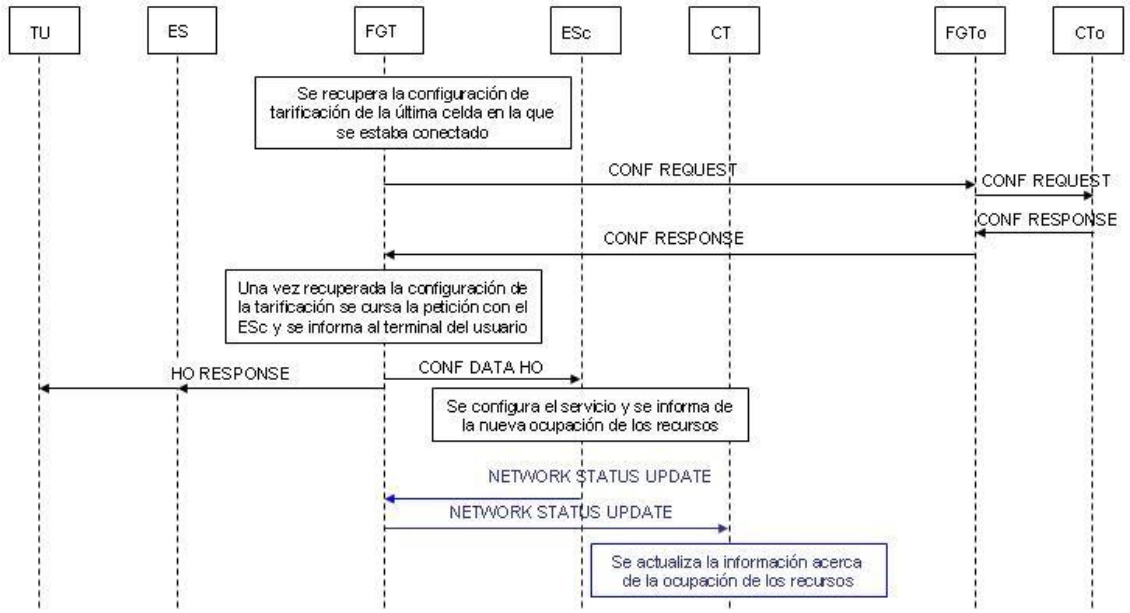


Figura 4.18 – Señalización cuando se escoge Esc para cursar una petición de traspaso

3.4 Parámetros utilizados en la simulación

Para el análisis del impacto del proceso de AA y el rendimiento general del protocolo utilizaremos el programa OMNET++, mediante el cuál simularemos eventos discretos desarrollados en C/C++ con los siguientes parámetros de simulación:

3.4.1 Parámetros generales de tráfico

General	
Tiempo de simulación	5 horas
Tipo de tráfico de llegada	Ráfagas
Tamaño de ráfagas (peticiones/ráfaga)	10 – 100
Tiempo entre cada petición de ráfaga	Exponencial (5.0)
Tiempo entre cada petición dentro de la ráfaga	Exponencial (0.1)
Distribución de la población de servicio	Voz → 62 %, Datos → 38 %
Tasa de traspasos	60 %
Tasa de nuevos servicios	40 %

El rango de 10 – 100 peticiones/ráfaga abarca desde el caso de tráfico insignificante a la casi congestión de la red. De esta manera se pretende evaluar como reacciona el sistema cuando las cosas van mal y la red se empieza a saturar.

3.4.2 Parámetros de retardos en enlaces (propagación y transmisión de datos)

Radioenlaces	
UMTS	
Retardo acceso	22.14 ms

El retardo considerado en el acceso a la red UMTS se considerará *ideal*, es decir, no se tendrán en cuenta los retardos introducidos por los reintentos de conexión ni tampoco se considerará ningún límite en la capacidad del acceso UMTS, es decir, por muy grande que sea el volumen de peticiones, el acceso UMTS no rechazará ninguna. El rechazo se realizará más adelante, bien en las celdas que prestarán el servicio o bien en la FGT, al comprobar ésta que no hay ninguna celda que pueda servir la petición recibida al estar todas ocupadas. Además, el retardo de propagación en los radio enlaces se considerará despreciable en comparación con el retardo de acceso.

Cableado	
Tamaño paquetes promedio	250 bytes
Velocidad de señalización rápida	2 Mbps
Retardo de transmisión promedio en canales rápidos	1 ms
Velocidad de señalización lenta	64 Kbps
Retardo de transmisión promedio en canales lentos	34 ms

El retardo de propagación del cableado también se considera despreciable en comparación con los retardos de transmisión.

Tal y como se ha podido observar en la tabla anterior, en las simulaciones realizadas se utilizarán dos tipos de retardos de transmisión en la señalización entre dominios de gestión diferentes. Por una parte se obtendrán los retardos promedios y los porcentajes de rechazos con el uso de canales de señalización de 64 Kbps (canales lentos) y por otro lado con canales de señalización de 2 Mbps (canales rápidos).

3.4.3 Parámetros de retardos de procesado de las entidades funcionales

	Procesado
ES	0.4 μs – 1.2 ms
FGT	2 – 10 μs
SM	0.4 μs - 1.2 ms
CT	3.06 – 3.50 ms
AA	0.4 μs - 1.2 ms

NOTA: La obtención de los retardos de procesado de cada una de las entidades funcionales y los parámetros generales del tráfico se encuentran detallados en el Anexo 2.

4 Resultados finales

A través de las gráficas que se mostrarán a continuación referentes a los resultados obtenidos, sacaremos conclusiones acerca del rendimiento del protocolo propuesto dentro de la arquitectura basada en políticas para la gestión de la tarificación en un ambiente de red de telecomunicaciones móviles avanzadas diseñada.

4.1 Retardo promedio de traspaso

A continuación se muestra la gráfica comparativa de los distintos retardos promedio en la ejecución de un traspaso según si la celda elegida pertenece o no al HO, si se realiza una AA en paralelo o en serie y si el canal de señalización es de 64 Kbps o de 2 Mbps.

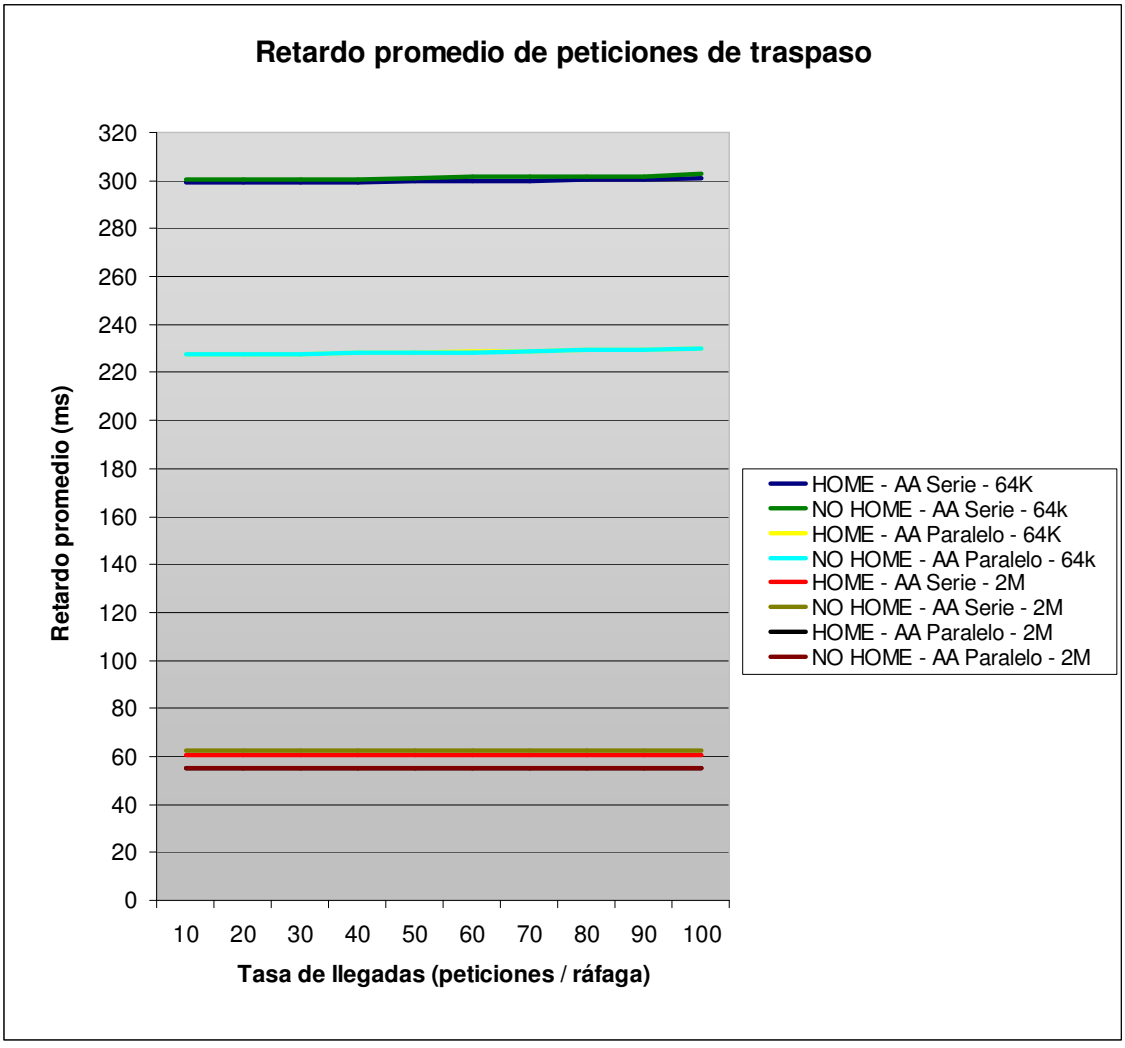


Figura 5.1 – Retardo promedio de peticiones de traspaso

Del gráfico podemos obtener las siguientes conclusiones:

1 – Cuando se realiza la AA en paralelo, las mejoras en cuanto al retardo promedio respecto a la AA en serie son bastante considerables:

- Celda pertenece al HO – 64 Kbps: reducción de 21,5 – 24 %
- Celda no pertenece al HO – 64 Kbps: reducción de 22 – 24 %
- Celda pertenece al HO – 2 Mbps: reducción de aprox. 9 %
- Celda no pertenece al HO – 2 Mbps: reducción de aprox. 11 %

Las variaciones en los porcentajes de reducción del retardo en un mismo escenario son debidos a que se han tenido en cuenta las reducciones producidas tanto en valores máximos como en valores promedio. De todas formas, estas variaciones porcentuales no sobrepasan el 2,5%, y en relación al total no son muy significativas. Como se puede comprobar a la vista de los resultados, el hecho de utilizar una AA en paralelo nos permite obtener unas reducciones del retardo promedio bastante considerables, sobretodo en las arquitecturas con canales de señalización a 64 Kbps. Esta reducción del retardo promedio de traspaso es debida a que en la AA en paralelo una vez se ha escogido la mejor celda para prestar el servicio, se ejecutan simultáneamente la AA y la configuración de la celda para cursar la petición. Esto tiene la ventaja de que el usuario puede empezar a disfrutar del servicio antes de haberse realizado por completo la AA, ya que el sistema no espera a que ésta sea satisfactoria para configurar los dispositivos implicados y proveer el servicio, y por lo tanto el retardo para la ejecución del traspaso se reduce considerablemente. El único pero que tiene este método es que en el caso de que la AA fuera insatisfactoria, el usuario podría haber estado disfrutando de los servicios sin que estuviera autorizado para ello, considerándose un pequeño "agujero" de seguridad. De todas formas, el hecho de que el usuario ya se encontrara dentro de la red, da por supuesto que ya había un mínimo de confianza entre el operador y el usuario, reduciendo a casos aislados el "agujero" de seguridad anteriormente mencionado. Como conclusión de los resultados, podríamos considerar que la relación seguridad/retardo con la AA en paralelo merece más la pena que en el caso de la AA en serie.

2 – El hecho de que la celda escogida mediante el algoritmo de selección pertenezca al HO del usuario o no introduce un retardo adicional debido a la necesidad de más mensajes en el proceso de señalización que concierne al caso de no pertenecer al HO. En este caso, la AA se deberá de realizar con los datos que almacenaba la última celda en la que había estado conectado el usuario, lo que supone un proceso más largo respecto al caso de autentificarse con el propio HO. En el caso de una petición de traspaso este procedimiento es del todo correcto, ya que el TU proviene de una red anterior, y se puede recuperar fácilmente la información referente a la AA, pero en el caso de una petición de nuevo servicio esto es menos correcto, ya que el usuario parte de cero, sin proceder de ningún sitio. Por tal de equiparar los dos casos, traspaso y nuevo servicio, se ha considerado que el procedimiento a seguir en cuanto a la AA en celdas que no pertenecen al HO en el caso de recibir una petición de nuevo servicio es el mismo que en el caso de una petición de traspaso, aunque ya hemos comentado

anteriormente que no es del todo correcto. Finalmente, las diferencias de retardo a la hora de procesar las peticiones en los caso de estar o no conectados al HO son las siguientes:

- Celdas en HO vs no HO – 64 Kbps: reducción de aprox. 0,5 %
- Celdas en HO vs no HO – 2 Mbps: reducción de aprox. 2 %

Como se puede observar, los resultados nos indican que las diferencias no son muy significativas. Cabe tener en cuenta que en el caso de realizar una AA en paralelo las diferencias en los retardos serían nulas, ya que las únicas diferencias en la señalización en los casos de pertenecer o no al HO se producen durante el proceso de AA, y no durante la configuración del servicio. Otro detalle a considerar es que estas diferencias dependerán mucho de la velocidad al ejecutar los cálculos o al procesar los mensajes por parte de la red anterior, ya que en esta fase es en donde radica la diferencia de retardos. Por lo tanto, si la red anterior es rápida, ya sea en procesamiento de mensajes, en señalización o en cálculo computacional, la diferencia se notará menos, y si es lenta, más.

3 – La utilización de canales de señalización de 2 Mbps reduce drásticamente el retardo promedio del proceso de traspaso. A continuación se muestran los porcentajes de reducción del retardo que se consiguen con el uso de los canales de señalización de 2 Mbps en cada uno de los casos estudiados:

- Celda pertenece al HO – AA Serie: reducción de 79,5 – 81 %
- Celda no pertenece al HO – AA serie: reducción de 79,5 – 80,5 %
- Celda pertenece al HO – AA paralelo: reducción de 75,5 – 78 %
- Celda no pertenece al HO – AA paralelo: reducción de 75,5 – 78 %

Las variaciones en los porcentajes de reducción del retardo son debidos a que se han tenido en cuenta las reducciones producidas tanto en valores máximos como en valores promedio. De todas formas, estas variaciones porcentuales no sobrepasan el 2,5 %, y en relación al total no son muy significativas. Mirando los resultados se puede ver claramente que el uso de canales de señalización más rápidos reduce drásticamente el retardo en el proceso de señalización del traspaso, por lo tanto, es una mejora muy a tener en cuenta de cara a la optimización del rendimiento del sistema.

4 – El hecho de aumentar la tasa de llegadas no influye en la variación del retardo total que se produce en la ejecución del proceso de traspaso. Esto es debido a que en el cómputo del retardo promedio del sistema sólo se han tenido en cuenta las peticiones que fueron cursadas, y tampoco se tuvo en cuenta ningún tipo de retardo adicional debido a los reintentos para obtener canal en el enlace radio. El impacto del aumento de la tasa de llegadas se verá reflejado cuando se analicen las gráficas de los porcentajes de peticiones rechazadas.

4.2 Retardo promedio de nuevos servicios

A continuación se muestra la gráfica comparativa de los distintos retardos promedio en el tratamiento de una petición de nuevo servicio según si la celda elegida pertenece al HO, si se realiza una AA en paralelo o en serie y si el canal de señalización es de 64 Kbps o de 2 Mbps.

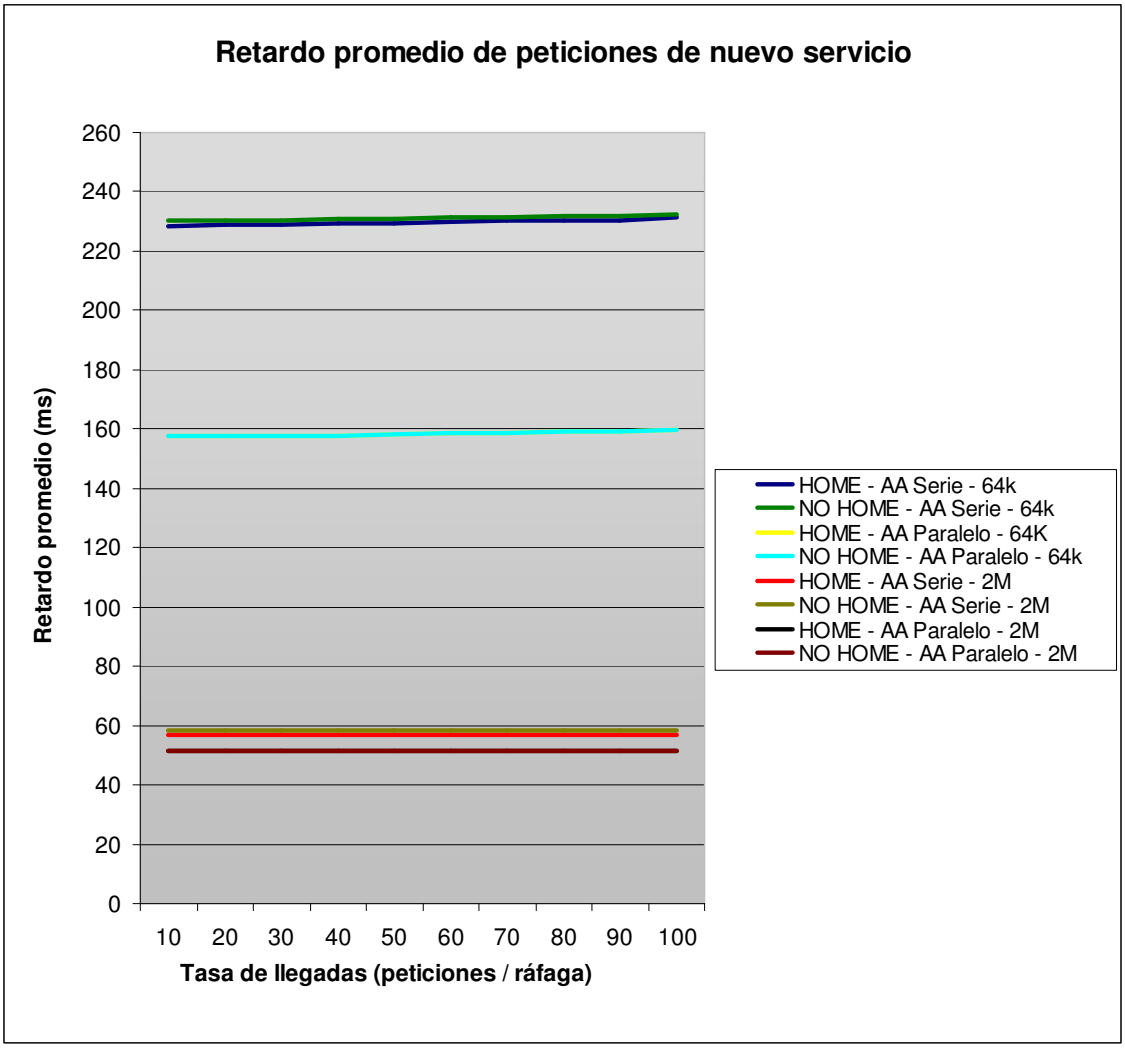


Figura 5.2 – Retardo promedio de peticiones de nuevo servicio

Del gráfico podemos obtener las siguientes conclusiones:

1 – Cuando se realiza la AA en paralelo, las mejoras en cuanto al retardo promedio respecto a la AA en serie son bastante considerables:

- Celda pertenece al HO – 64 Kbps: reducción de 27,5 – 31 %
- Celda no pertenece al HO – 64 Kbps: reducción de 28 – 31,5 %
- Celda pertenece al HO – 2 Mbps: reducción de aprox. 9,5 %
- Celda no pertenece al HO – 2 Mbps: reducción de aprox. 12 %

Las variaciones en los porcentajes de reducción del retardo son debidos a que se han tenido en cuenta las reducciones producidas tanto en valores máximos como en valores promedio. De todas formas, estas variaciones porcentuales no sobrepasan el 3,5 % en los casos más significativos, y en relación al total no son muy significativas. Como se puede comprobar a la vista de los resultados, el hecho de utilizar una AA en paralelo nos permite obtener unas reducciones del retardo promedio bastante considerables, sobretodo en las arquitecturas con canales de señalización a 64 Kbps. Esta reducción del retardo promedio de traspaso es debida a que en la AA en paralelo una vez se ha escogido la mejor celda para prestar el servicio, se ejecutan simultáneamente la AA y la configuración de la celda para cursar la petición. Esto tiene la ventaja de que el usuario puede empezar a disfrutar del servicio antes de haberse realizado por completo la AA, ya que el sistema no espera a que ésta sea satisfactoria para configurar los dispositivos implicados y proveer el servicio, y por lo tanto el retardo para la ejecución del traspaso se reduce considerablemente. El único pero que tiene este método es que en el caso de que la AA fuera insatisfactoria, el usuario podría haber estado disfrutando de los servicios sin que estuviera autorizado para ello, considerándose un pequeño "agujero" de seguridad. De todas formas, el hecho de que el usuario ya se encontrara dentro de la red, da por supuesto que ya había un mínimo de confianza entre el operador y el usuario, reduciendo a casos aislados el "agujero" de seguridad anteriormente mencionado. Como conclusión de los resultados, podríamos considerar que la relación seguridad/retardo con la AA en paralelo merece más la pena que en el caso de la AA en serie.

2 – El hecho de que la celda escogida mediante el algoritmo de selección pertenezca al HO del usuario o no introduce un retardo adicional debido a la necesidad de más mensajes en el proceso de señalización que concierne al caso de no pertenecer al HO. En este caso, la AA se deberá de realizar con los datos que almacenaba la última celda en la que había estado conectado el usuario, lo que supone un proceso más largo respecto al caso de autentificarse con el propio HO. En este caso, al tratarse de una petición de nuevo servicio, no tiene del todo sentido el hecho de recuperar los datos de autentificación de la última celda a la que se estuvo conectado, ya que la petición es nueva, y el concepto de celda anterior no existe. De todas formas por tal de equiparar los dos casos, traspaso y nuevo servicio, se ha considerado que el procedimiento a seguir en cuanto a la AA en celdas que no pertenecen al HO en el caso de recibir una petición de nuevo servicio es el mismo que en el caso de una petición de traspaso, aunque ya hemos comentado anteriormente que no es del todo correcto. Finalmente, las diferencias de retardo a la hora de procesar las peticiones en los casos de estar o no conectados al HO son los siguientes:

- Celdas en HO vs no HO – 64 Kbps: reducción de aprox. 0,5 – 0,75 %
- Celdas en HO vs no HO – 2 Mbps: reducción de aprox. 2,5 %

Como se puede observar, los resultados nos indican que las diferencias no son muy significativas. Cabe tener en cuenta que en el caso de realizar una AA en paralelo las diferencias en los retardos serían nulas, ya que las únicas diferencias en la señalización en los casos de pertenecer o no al HO se producen durante el proceso de AA, y no durante la configuración del servicio. Otro detalle a considerar es que estas diferencias dependerán mucho de la velocidad al ejecutar los cálculos o al procesar los mensajes por parte de la red anterior, ya que en esta fase es en donde radica la diferencia de retardos. Por lo tanto, si la red anterior es rápida, ya sea en procesamiento de mensajes,

en señalización o en cálculo computacional, la diferencia se notará menos, y si es lenta, más.

3 – La utilización de canales de señalización de 2 Mbps reduce considerablemente el retardo promedio del proceso de traspaso. A continuación se muestran los porcentajes de reducción del retardo que se consiguen con el uso de los canales de señalización de 2 Mbps en cada uno de los casos estudiados:

- Celda pertenece al HO – AA Serie: reducción de 79,5 – 81 %
- Celda no pertenece al HO – AA serie: reducción de 79,5 – 80,5 %
- Celda pertenece al HO – AA paralelo: reducción de 75,5 – 78 %
- Celda no pertenece al HO – AA paralelo: reducción de 75,5 – 78 %

Las variaciones en los porcentajes de reducción del retardo son debidos a que se han tenido en cuenta las reducciones producidas tanto en valores máximos como en valores promedio. De todas formas, estas variaciones porcentuales no sobrepasan el 2,5 %, y en relación al total no son muy significativas. Mirando los resultados se puede ver claramente que el uso de canales de señalización más rápidos reduce drásticamente el retardo en el proceso de señalización del traspaso, por lo tanto, es una mejora muy a tener en cuenta de cara a la optimización del rendimiento del sistema.

4.3 Distribución de los retardos

Tal y como se ve en las tablas de resultados (Anexo 1), en cada simulación los retardos tenían una desviación estándar, la cuál rondaba los 30 ms en el caso de los canales de señalización de 64 Kbps y 1 ms en el caso de los canales de señalización de 2 Mbps. Estás desviaciones son debidas únicamente a la diferencia de retardos en la señalización entre cuando se escoge la celda en la que ya se estaba conectado (Esc) o cuando se escoge cualquier otra de las 3 celdas en las que no se estaba conectado (Esn). Con los canales de 64 Kbps esta diferencia de retardo será mayor al ser los canales más lentos a la hora de transmitir los mensajes. Por lo tanto, la distribución de retardos se concentra en dos picos, uno para el retardo que se produce cuando la celda seleccionada es la Esc y otro para cuando las celdas seleccionadas son Esn, con n=1,2 y 3.

4.4 Peticiones rechazadas

A continuación, en este apartado se analizarán detenidamente los resultados obtenidos en cuanto a los porcentajes de peticiones rechazadas según la tasa de llegadas que tiene el sistema y según dónde se producen estos rechazos. Las peticiones pueden ser rechazadas en dos entidades diferentes, en la FGT y en el Esx.

1 – *Rechazo en la FGT:* Se produce cuando se recibe una petición, ya sea de traspaso o de nuevo servicio, y la FGT ya tiene constancia de que todas las redes a las que tiene acceso están totalmente ocupadas y no les queda ningún recurso para servir más peticiones. Entonces, la petición es rechazada en la FGT y ni siquiera se ejecuta el algoritmo de selección de celda.

2 – *Rechazo en el Esx:* Se produce cuando las redes a las que tiene conexión la FGT están rozando el máximo de capacidad y la FGT cursa peticiones que realmente luego no podrán ser servidas, ya que cuando llegan al Esx, éste resulta estar al máximo de su capacidad. Esto sucede porque las actualizaciones de disponibilidad de recursos que se reciben del CT no están actualizadas en tiempo real, entonces cuando se rozan los límites del máximo de capacidad en las redes y la tasa de llegadas es muy alta, resulta que la FGT puede ejecutar el algoritmo de selección de celda a dos peticiones en un corto intervalo de tiempo sin que se haya actualizado la información que tiene el CT de los recursos ocupados por las redes. Esto da lugar a que alguna de las peticiones a las que se le ha asignado una celda, cuando lleguen al Esx no tengan recursos para ser servidas y sean rechazadas. Si el CT tuviera la información de los recursos disponibles actualizada en tiempo real, los rechazos se producirían únicamente en la FGT, pero al no ser así, en la realidad tendremos rechazos también en los Esx.

A continuación, una vez definidos los tipos de rechazos que se pueden producir, pasaremos a estudiar las distintas gráficas en referencia a ellos. Para tener una idea más clara de lo que está pasando se presentarán diferentes gráficas en función del tipo de petición rechazada y de la entidad en la cual se produce el rechazo. Estas gráficas mostrarán el porcentaje de peticiones rechazadas para los casos anteriormente estudiados de AA en serie y en paralelo, canales de señalización de 64 Kbps o 2 Mbps y celdas escogidas pertenecientes o no al HO.

4.4.1 Peticiones rechazadas totales

La primera gráfica que se mostrará será la de peticiones totales rechazadas, la cual engloba los casos de peticiones de traspaso y de nuevo servicio rechazadas, ya sea en la FGT o en el Esx.

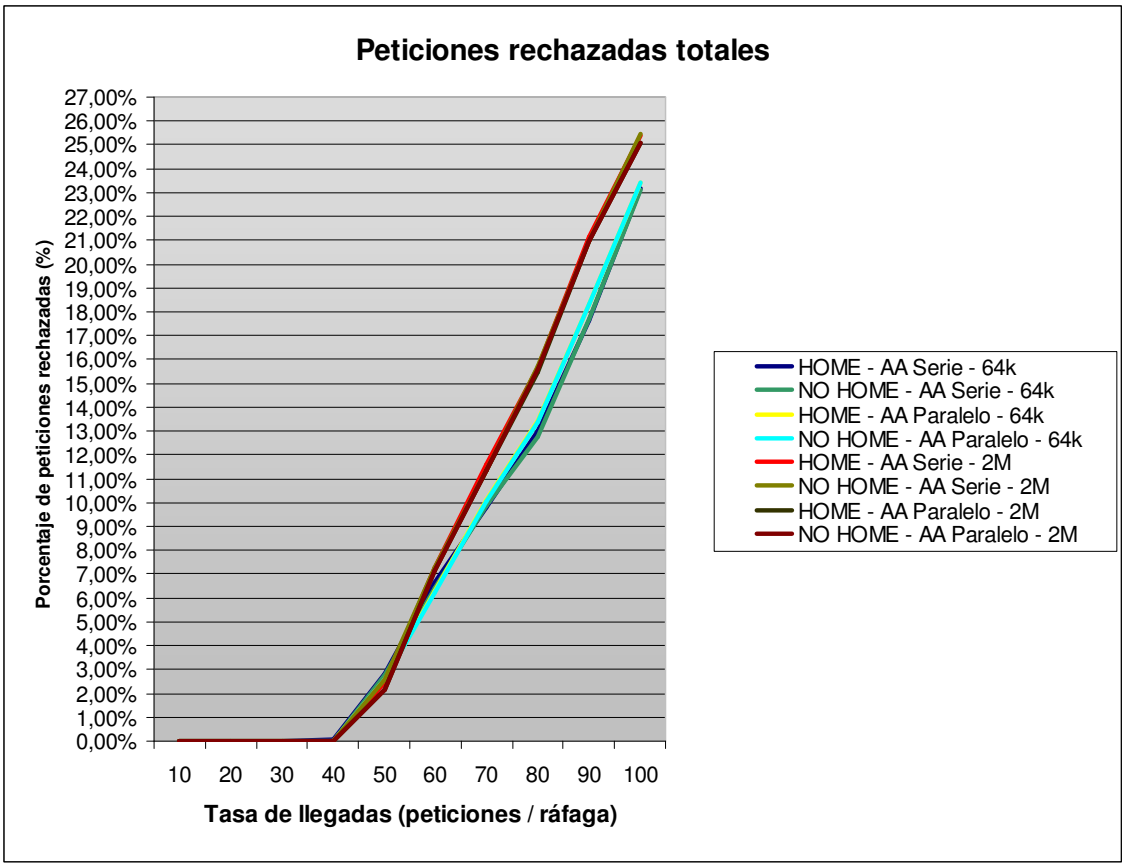


Figura 5.3 – Peticiones rechazadas totales

Tal y como se puede observar en la gráfica, el porcentaje de peticiones rechazadas es casi independiente del tipo de autentificación utilizado y de si la celda escogida pertenece o no al HO. Los dos factores determinantes del porcentaje de peticiones rechazadas son la velocidad del canal de señalización y la tasa de llegadas de las peticiones. En la gráfica se observa claramente el punto a partir del cual empiezan a rechazarse las peticiones, concretamente se trata de 40 peticiones/ráfaga. También se puede observar que a partir de las 60 peticiones/ráfaga los rechazos en los casos de canales de señalización de 64 Kbps y 2 Mbps se empiezan a separar y que con 2 Mbps tenemos entre un 1 – 2,5 % más de rechazos que con 64 Kbps. Otro detalle a tener en cuenta es la pendiente de las rectas, ya que se pueden diferenciar dos tramos a partir de las 40 peticiones/ráfaga. Estos tramos son de 50-80 peticiones/ráfaga y de más de 80 peticiones/ráfaga. Las pendientes de los diferentes tramos, considerando las dos velocidades de señalización son las siguientes:

Velocidad señalización	***Tramo 50-80 pet/ráfaga***	***Tramo de +80 pet/ráfaga***
64 Kbps	0,34	0,52
2 Mbps	0,43	0,47

Por los resultados obtenidos se puede deducir lo siguiente:

1 – El porcentaje de peticiones rechazadas va aumentando exponencialmente a medida que la tasa de llegadas crece.

→ Esto es debido a que cuando se consume toda la capacidad de servicio que tiene la red, las siguientes peticiones que vengan se irán rechazando hasta que no se libere algún canal o parte del ancho de banda ocupado. Entonces, a medida que aumenta la tasa de llegadas, el porcentaje de peticiones rechazadas va creciendo exponencialmente ya que los elementos de servicio (ES) están constantemente al máximo de capacidad y los recursos se van liberando muy poco a poco en comparación con la avalancha de peticiones que reciben.

2 – A mayor velocidad de señalización, mayor porcentaje de peticiones rechazadas a igual tasa de llegadas.

→ Esto es debido a que al ser los canales de señalización más rápidos, los elementos de servicio (ES) reciben las peticiones con menor retraso, ya que los retardos de transmisión entre las distintas entidades funcionales se reducen considerablemente. Esto hace que desde que todos los recursos están ocupados hasta que se produce la siguiente liberación de algún recurso se rechacen muchas más peticiones que en el caso de enlaces de señalización más lentos. Por lo tanto, a igual tasa de llegadas que en el caso de la señalización más lenta, las peticiones rechazadas son mayores. Esta diferencia entre los dos canales de señalización a distintas velocidades se verá reducida conforme la tasa de llegadas vaya aumentando más, ya que se llegará a un punto en el que todas las peticiones recibidas serán rechazadas por incapacidad del sistema ante tanto tráfico.

4.4.2 Peticiones rechazadas totales en la FGT y en el Esx

A continuación se analizan las peticiones rechazadas totales, pero sólo las que se producen en la FGT y en el Esx de forma separada.

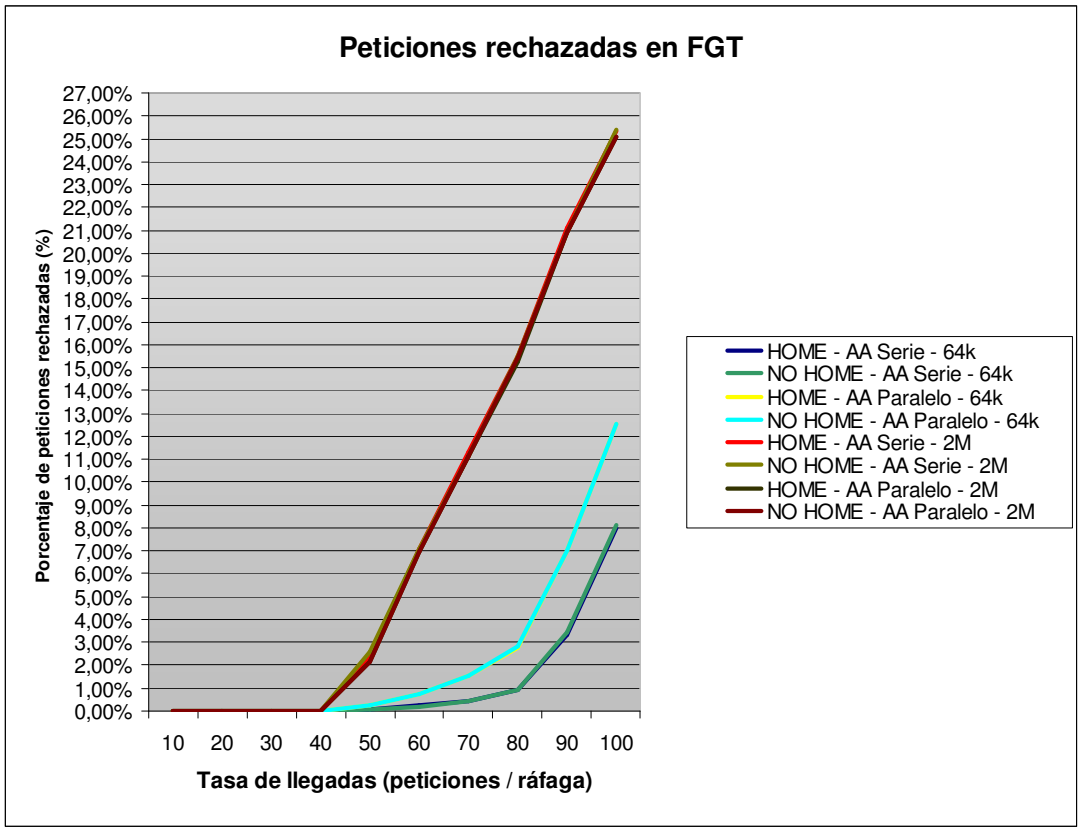


Figura 5.4 – Peticiones rechazadas en FGT

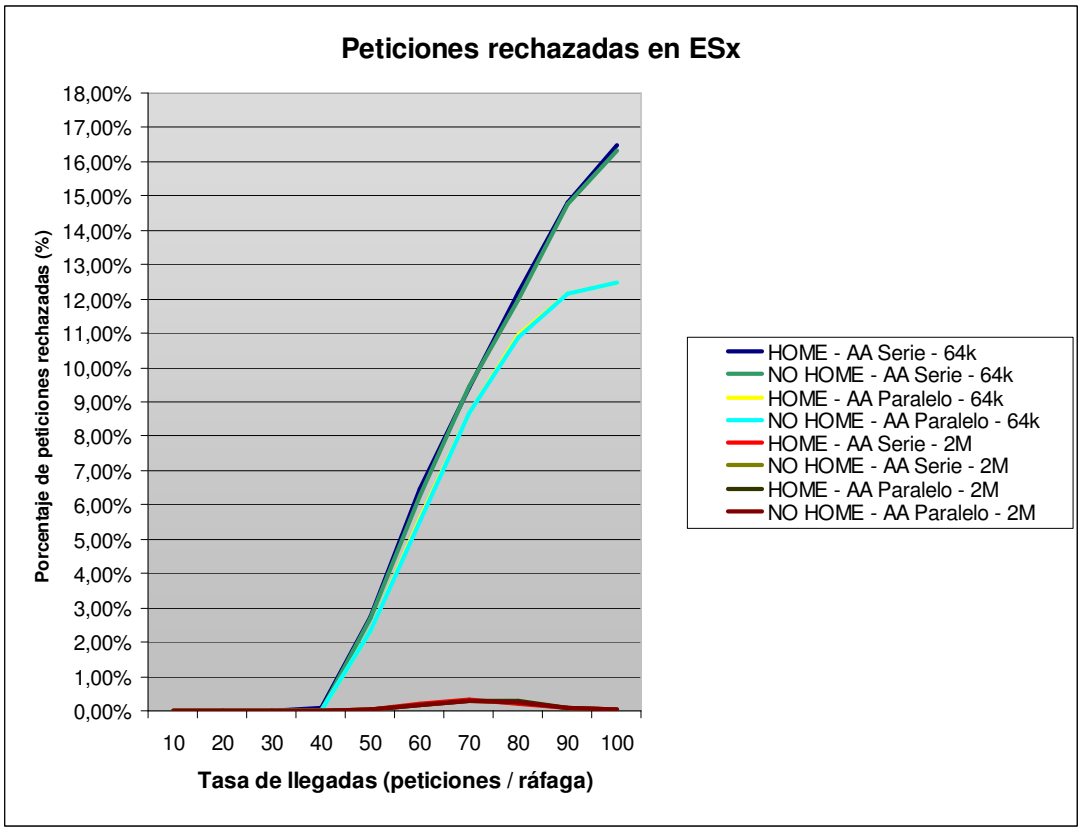


Figura 5.5 – Peticiones rechazadas en Esx

En estas gráficas llama mucho la atención el hecho de que haya una gran diferencia entre las peticiones rechazadas cuando se utilizan canales de señalización de 64 Kbps y 2 Mbps. En el caso de los canales de 2 Mbps, la gráfica de peticiones rechazadas en la FGT es casi idéntica a la gráfica anteriormente mostrada de peticiones rechazadas totales y en el Esx los rechazos son casi 0 %. En cambio, para los canales de 64 Kbps las gráficas son totalmente diferentes al caso general de peticiones rechazadas totales. A continuación se analizarán detenidamente los motivos de estas diferencias:

Canales de 64 Kbps

Rechazos en la FGT

En este caso los porcentajes de peticiones rechazadas difieren mucho del global, esto es debido a que con los canales de 64 Kbps hay más probabilidad de que al llegar al Esx éste ya esté totalmente ocupado. Esto es debido a que al ser canales más lentos, la actualización de la ocupación de recursos que llega al CT requiere más tiempo, y entonces estas actualizaciones no son en tiempo real, lo que conlleva a que en el momento de recibir una petición y ejecutar el algoritmo de selección de celda, la FGT no disponga de la información actualizada. Por este motivo, en el intervalo de entre 40-80 peticiones/ráfaga la mayoría de los rechazos se producen en el Esx, ya que constantemente se producen los errores de asignación de celdas debido a la no actualización en tiempo real de la disponibilidad de recursos. A partir de 80 peticiones/ráfaga, el sistema está tan saturado que aunque la actualización difiera bastante del tiempo real, está tan ocupado que en el momento de llegar la petición a la FGT ésta es informada de que no hay más recursos para servir las peticiones y decide rechazar la petición.

Además de lo anteriormente mencionado, también se aprecia una diferencia entre las peticiones rechazadas cuando se utiliza AA en serie y AA en paralelo. Concretamente, con la AA en paralelo se producen más rechazos en la FGT que con la AA en serie. Esto es debido a que en el caso de la AA en paralelo las actualizaciones de la disponibilidad de los recursos se realizan antes que en el caso de la AA en serie, porque en el primer caso las peticiones se sirven antes que en el segundo y por lo tanto, la información que envían los Esx al CT con la ocupación de sus recursos se recibe antes que en el caso de la AA en serie.

Rechazos en el Esx

En la Esx, igual que en el caso de los rechazos en la FGT, los resultados difieren mucho del global, ya que el global es la suma de los rechazos en la FGT y en el Esx y si uno difiere del global, el otro también. De los rechazos en el Esx poco se puede decir que no se haya dicho ya en el apartado anterior. El único detalle a comentar es que a partir de las 90 peticiones/ráfaga en el caso de la AA en paralelo y un poco más tarde en la AA en serie, los rechazos en la Esx se quedan estancados. Esto es debido a que con estas tasas de llegadas el sistema está tan saturado de tráfico que la gran mayoría de las peticiones se pueden rechazar ya en la FGT puesto que todos los recursos están ocupados.

Canales de 2 Mbps

Rechazos en la FGT

En este caso, los porcentajes de peticiones rechazadas son casi idénticos al global. Esto es debido a que al tener los canales de señalización más rápidos, el problema de la actualización de la información referente a los recursos de las redes no se produce, y por lo tanto, casi todos los rechazos se producen en la FGT, ya que ésta en el momento de llegar la petición dispone de la información actualizada de la capacidad libre que tienen las redes colindantes a ella.

Rechazos en el Esx

En este caso, al no producirse la desactualización de la información de la FGT en cuanto a la ocupación de recursos el porcentaje de rechazos es casi 0 %.

4.4.3 Peticiones rechazadas totales según el tipo de servicio solicitado

Las gráficas que se mostrarán a continuación nos enseñan como evoluciona el porcentaje de peticiones rechazadas globales según si las peticiones son de traspaso o de nuevo servicio.

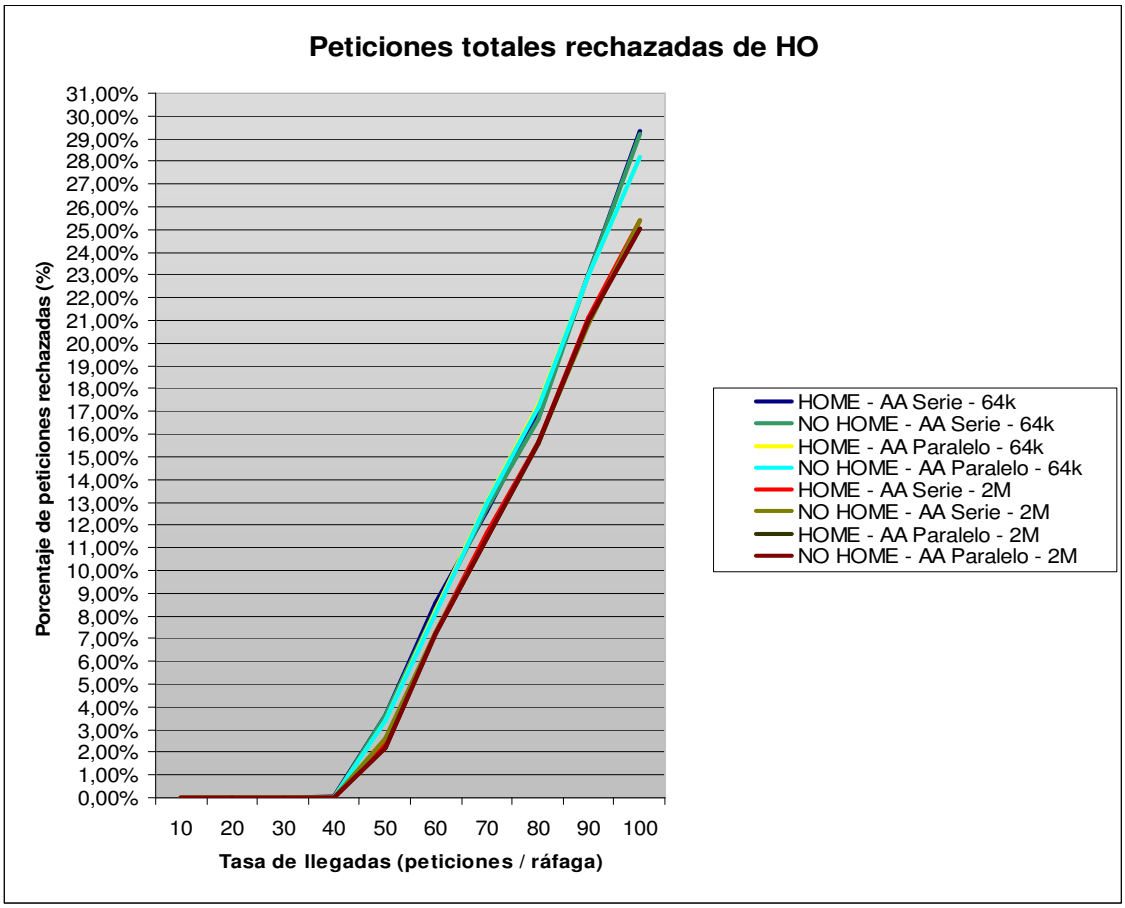


Figura 5.6 – Peticiones totales rechazadas de HO

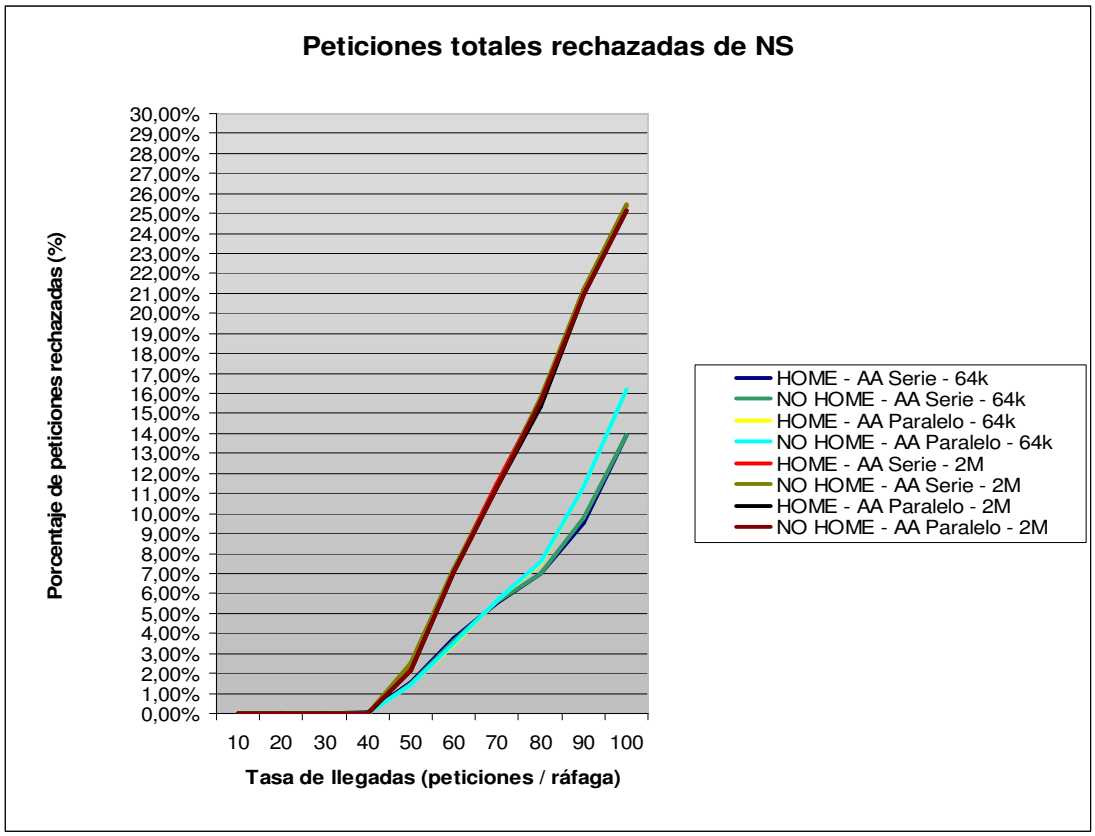


Figura 5.7 – Peticiones totales rechazadas de NS

En las gráficas anteriores hay bastantes detalles importantes para obtener conclusiones:

Peticiones totales rechazadas de traspaso

En la gráfica notamos una diferencia significante respecto a los porcentajes de rechazos cuando se usan canales de señalización de 64 Kbps y 2 Mbps. Nos llama especialmente la atención que a diferencia del caso global, en el cual no se tiene en cuenta el tipo de petición, en este caso cuando se usan canales de señalización de 64 Kbps se producen más porcentajes de rechazos que en el caso de canales de 2 Mbps. La explicación a esto la veremos cuando se analicen los porcentajes de rechazos según el tipo de petición y según la entidad donde se producen.

Peticiones totales rechazadas de nuevo servicio

Igual que en el caso anterior, se observa que la gráfica no se parece en nada a la del caso de peticiones rechazadas globales, sin tener en cuenta el tipo de petición. Para canales de señalización de 2 Mbps el porcentaje de peticiones rechazadas se mantiene en la misma línea que en el caso de las peticiones de traspaso rechazadas, pero cuando se trata de los canales de 64 Kbps, no tienen nada que ver el uno con el otro. Con canales de 64 Kbps las peticiones de nuevo servicio rechazadas son mucho menores que las peticiones de traspaso, y si nos fijamos en gráficas anteriores, la gráfica de los rechazos de peticiones de nuevos servicios con canales de 64 Kbps se parece mucho a la gráfica de peticiones rechazadas en la FGT. La explicación a esto la veremos cuando se analicen los porcentajes de rechazos según el tipo de petición y según la entidad donde

se producen.

4.4.4 Peticiones rechazadas según el tipo de servicio en la FGT y en el Esx

A continuación, para acabar de analizar los motivos de las diferencias de porcentajes de rechazos según el tipo de servicio solicitado, analizaremos el porcentaje de rechazos según el tipo de petición y según si los rechazos se producen en la FGT o en el Esx.

Empezaremos analizando las peticiones rechazadas en la FGT, las cuales se mostrarán en las siguientes gráficas:

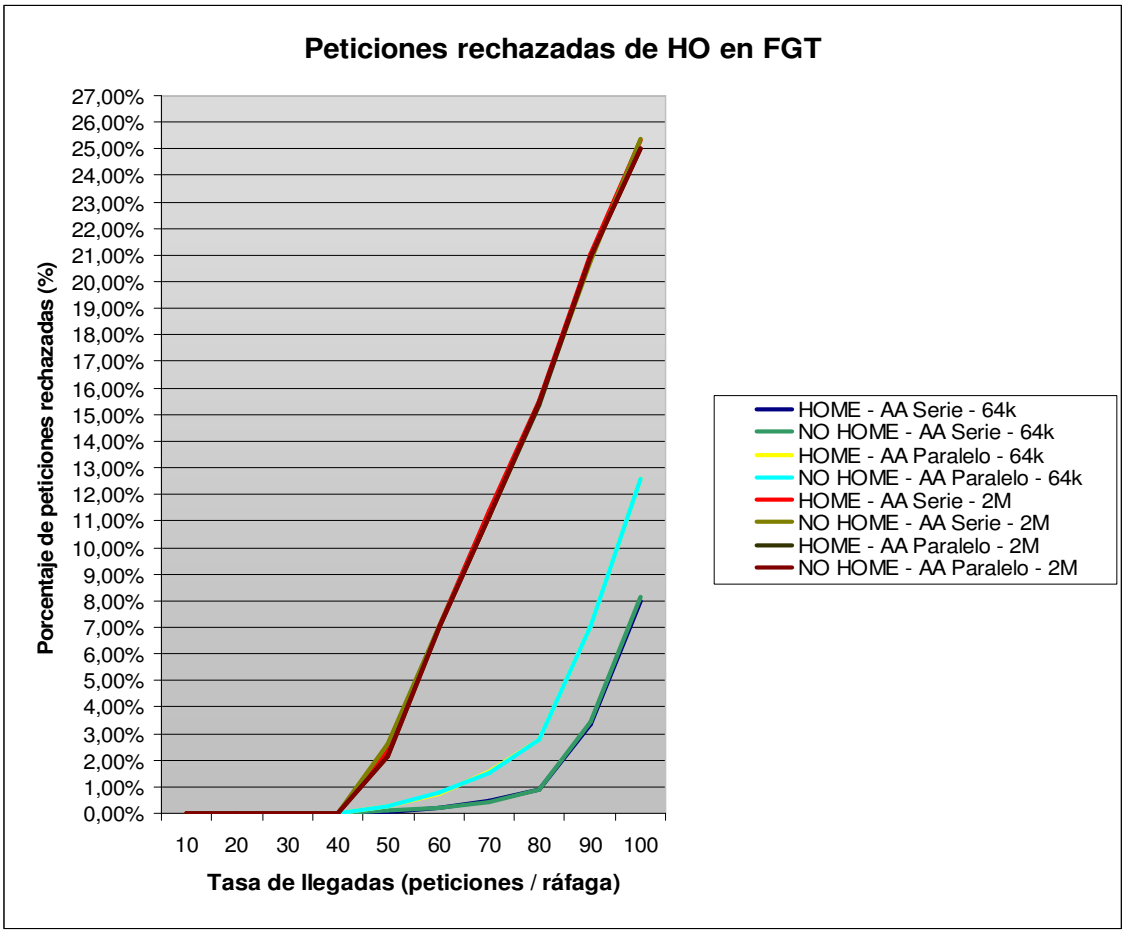


Figura 5.8 – Peticiones rechazadas de HO en FGT

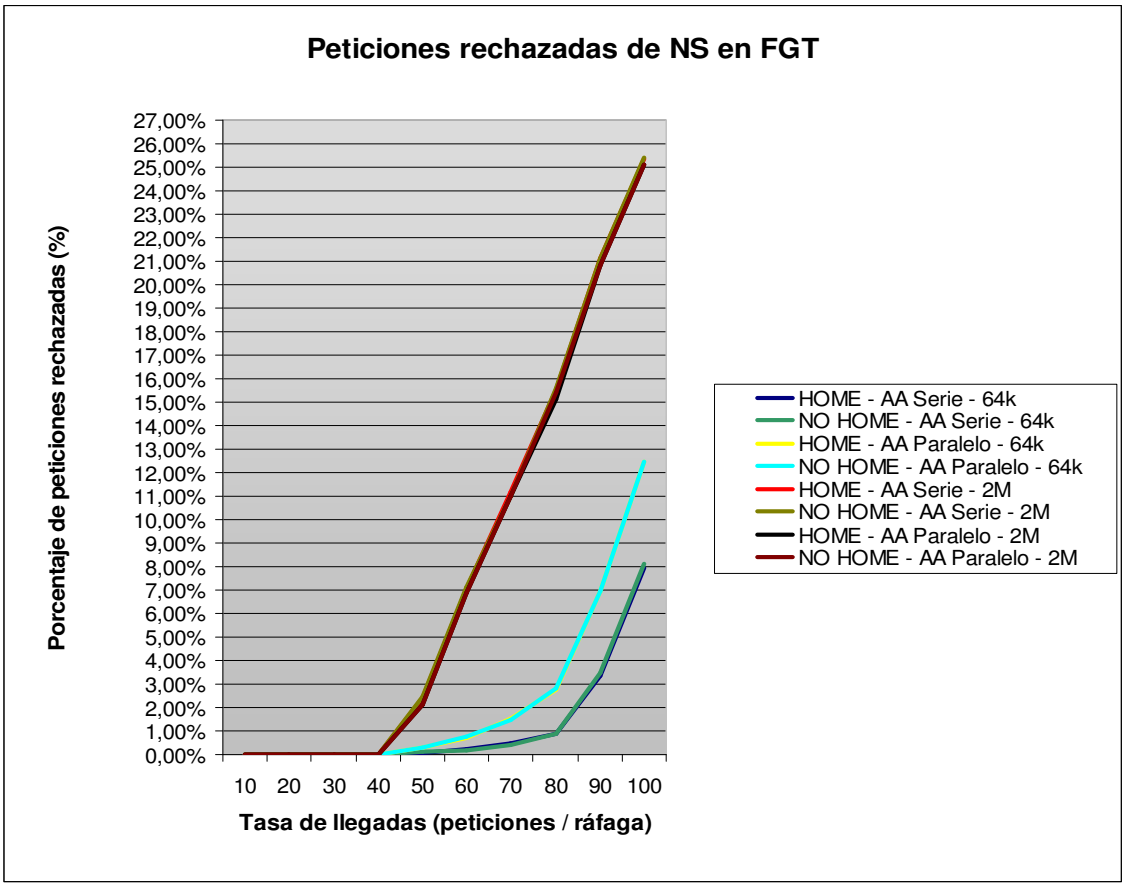


Figura 5.9 – Peticiones rechazadas de NS en FGT

Peticiones de traspaso y de nuevo servicio rechazadas en la FGT

En este caso observamos que el porcentaje de peticiones rechazadas es aproximadamente el mismo para el caso de las peticiones de traspaso y el de nuevos servicios, tanto para canales de señalización de 64 Kbps como para canales de 2 Mbps. Por lo tanto, en este caso no hay nada a comentar que no se haya comentado en apartados anteriores.

Finalmente analizaremos las peticiones rechazadas en el Esx según los resultados mostrados en las siguientes gráficas:

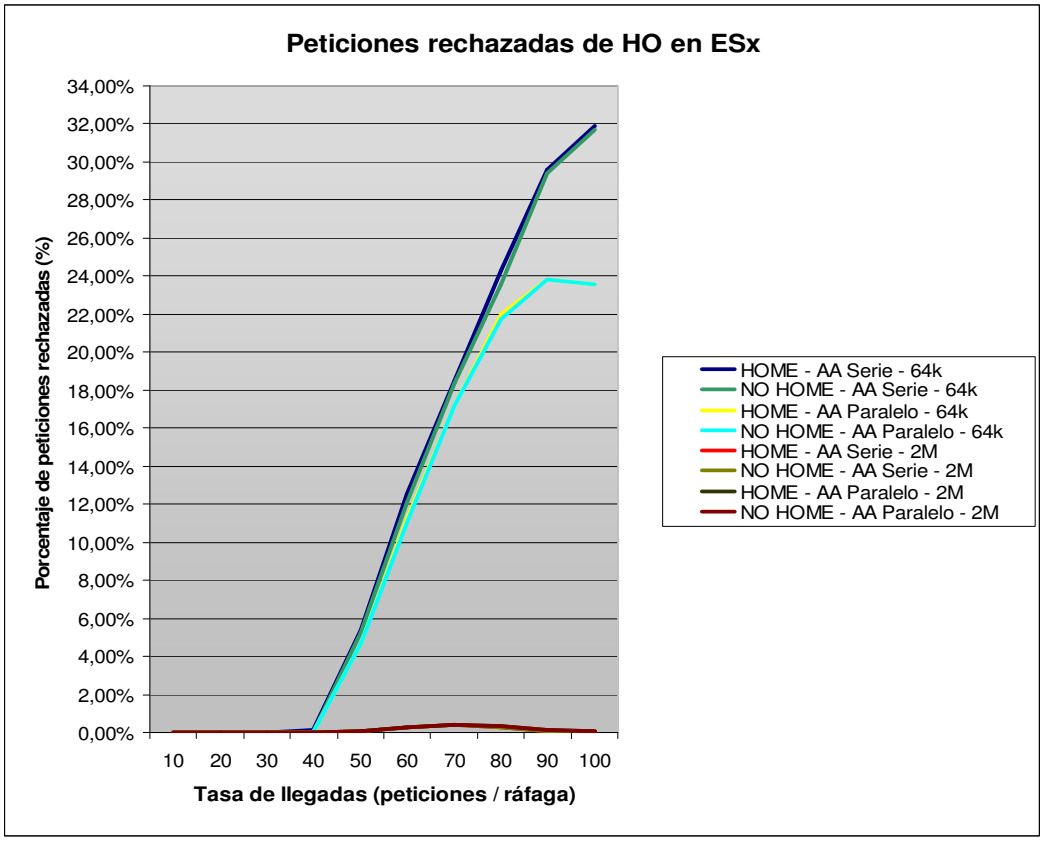


Figura 5.10 – Peticiones rechazadas de HO en Esx

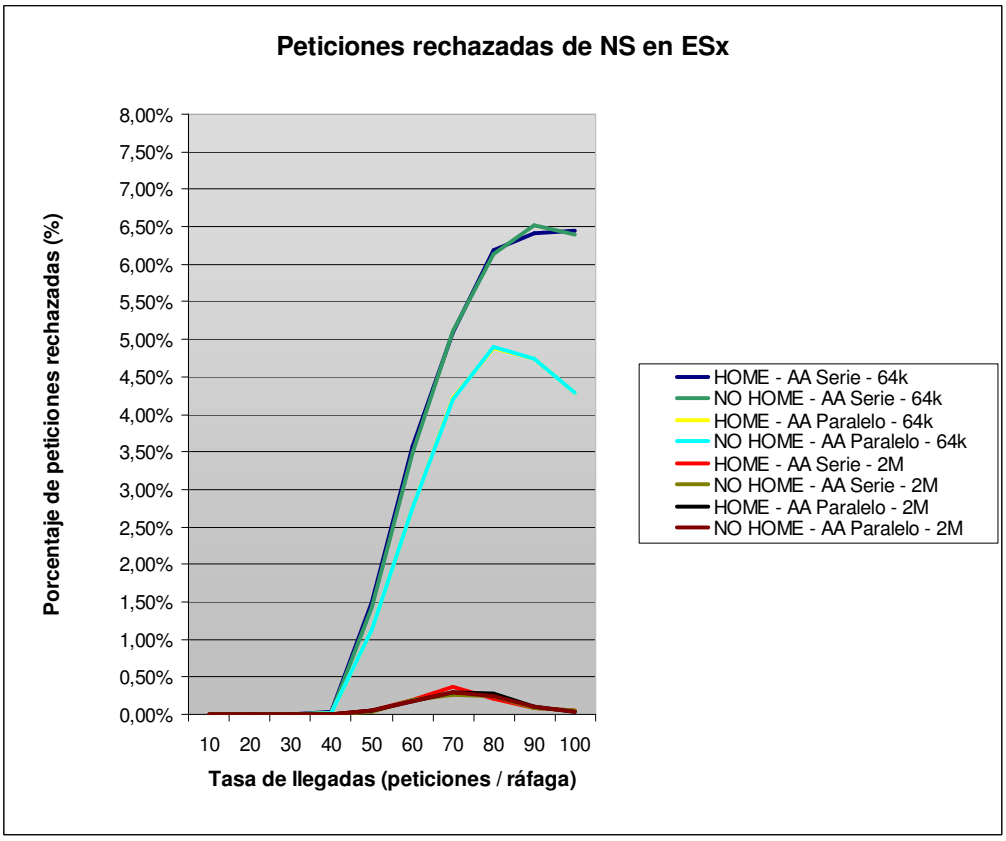


Figura 5.11 – Peticiones rechazadas de NS en Esx

Peticiones de traspaso y de nuevo servicio rechazadas en el Esx

Finalmente, en este apartado podemos encontrar la explicación a la diferencia del porcentaje de rechazos entre las peticiones de nuevo servicio y las peticiones de traspaso con canales de señalización de 64 Kbps. La diferencia proviene de los rechazos en el Esx, ya que en esta entidad se producen muchos más rechazos de peticiones de traspaso que de nuevo servicio. La explicación de todo esto es la siguiente:

Por el motivo comentado al principio, cuando se analizaban los porcentajes de peticiones rechazadas totales, existe un retardo en la actualización de la información referente a la ocupación de las celdas que hace que cuando se utilizan canales de señalización de 64 Kbps se cometan errores a la hora de asignar celdas para cursar la petición. El caso es que el algoritmo de selección de celda usa información no actualizada en tiempo real y entonces, con el uso de canales de señalización lentos, puede darse el caso de que asigne una celda a varias peticiones sin todavía saber que esta celda ya no tiene más capacidad. El problema de todo esto, y el motivo de la diferencia de peticiones rechazadas de traspaso y de nuevo servicio en el Esx, es que la señalización de un traspaso necesita más mensajes para llevarse a cabo que la señalización de un nuevo servicio, lo que da lugar a que llegadas de ambos tipos de servicio en un intervalo muy pequeño de tiempo hacen que este problema de la desactualización sea mucho más acusado en el caso de las peticiones de traspaso. El motivo es bien simple, y con un ejemplo se entiende mejor.

Ejemplo:

- Llegan en un corto intervalo de tiempo una petición de nuevo servicio y una de traspaso.

- La FGT tiene la información de la ocupación de recursos que le dice que sólo queda X BW (Bandwidth – Ancho de banda) libre para dar servicio a las peticiones recibidas, y que este BW pertenece a una única celda.

- La FGT ejecuta el algoritmo de selección de celda para la primera petición recibida, y escoge la única celda que tiene algo de BW para cursar peticiones. Acto seguido empieza la señalización para cursar la petición.

- La FGT ejecuta el algoritmo de selección de celda para la segunda petición recibida, y al no haberse actualizado aún la información de la ocupación de los recursos, ya que no ha dado tiempo a que la petición se curse y que la Esx informe de la nueva ocupación, selecciona otra vez la única celda que tenía X BW libre para dar servicio a las peticiones recibidas.

- A la hora de llegar al Esx, habrá dos peticiones para un mismo y único recurso, por lo tanto, la última que llegue será rechazada por el Esx. En el caso de que las peticiones fueran una de nuevo servicio y otra de traspaso, la petición de traspaso sería la última en llegar, ya que su señalización requiere más mensajes que en el caso del nuevo servicio, y por este motivo con canales de señalización de 64 Kbps hay muchas más peticiones de traspaso rechazadas en el Esx que peticiones de nuevo servicio.

5 Conclusiones

El incremento del número de necesidades que plantean las sociedades modernas a dado lugar a que debido a su complejidad, la gestión de red se haya convertido en un factor crucial para el éxito del ofrecimiento de nuevos servicios. El hecho de que el usuario necesite una mayor movilidad y un mayor número de posibilidades de conexión allá donde vaya hacen que se precise cada vez más de redes que proporcionen cobertura mundialmente.

Estas redes no tienen porque ser de un mismo operador, sino que pueden estar formadas por diferentes compañías que cooperan entre ellas mediante acuerdos para abarcar una mayor área de cobertura y ofrecer al usuario un abanico más amplio de servicios con todo tipo de tecnologías y sin ningún tipo de cortes a causa de la movilidad. Actualmente el usuario desea mantenerse informado, escuchar música, ver vídeos, hablar con los amigos, descargarse archivos, etc… en cualquier escenario.

Para satisfacer todas estas necesidades se precisan nuevos mecanismos de tarificación, recolección de información de eventos tarificables y modelos de facturación que nos permitan dar la flexibilidad necesaria en las comunicaciones para que una serie de parámetros de la red puedan ser modificados para cumplir el nivel de servicio que precisa el usuario en cada momento.

En este contexto es donde debe ubicarse nuestra propuesta de diseño de una arquitectura de gestión de la tarificación para un entorno de red de comunicaciones móviles avanzadas. Esta arquitectura no sólo nos debe permitir satisfacer las necesidades actuales, sino que también deberá preveer el soporte de futuras aplicaciones y tener en cuenta las nuevas tendencias de las sociedades actuales, las cuales son:

- **Movilidad.** Asociada a gente, ideas, información financiera, científica, documentos multimedia como vídeos, fotos, música, etc.

- **Simultaneidad.** Todo el mundo ha de estar disponible en cualquier lugar, en cualquier momento y con un amplio abanico de dispositivos y tecnologías.

- **Continuidad.** Los servicios proporcionados ya sea por los operadores de red o por los proveedores de servicio no deben de estar restringidos a una cierta área de cobertura sino que deben ser accesibles desde cualquier lugar, con cualquier tecnología y sin que el usuario note ningún tipo de perturbación en cuanto se desplaza mientras está disfrutando del servicio.

- **Competitividad.** La globalización debe permitir la competitividad entre fronteras y permitir varias alternativas en la selección de múltiples operadores de red y proveedores de servicio por parte de los usuarios. Además debe facilitar el acceso al mercado de otro tipo de proveedores de servicios de valor añadido que añadan nuevas aplicaciones y satisfagan las nuevas necesidades de los usuarios.

Por otra parte, los crecientes avances tecnológicos permiten diseñar escenarios de redes inteligentes con sistemas de gestión distribuidos basados en equipos informáticos de altas prestaciones capaces de soportar los altos requerimientos de cálculo de estas nuevas redes ambientales.

Las entidades de gestión proporcionan la información necesaria sobre el estado de la red, aportando datos sobre la congestión de ésta en cada momento. Además las bases de datos pueden almacenar desde perfiles de usuarios con sus respectivos parámetros de calidad de servicio requerida, servicios disponibles, tarifas aplicables, etc… hasta certificados de clave pública y todos los datos necesarios en cuanto a seguridad. Y en el apartado de los terminales inteligentes, ya sean móviles, PDA's, portátiles o cualquier otro dispositivo mediante el cual se tenga acceso a la red, permitirán soportar la gestión de claves y servicios de seguridad especificados, así como la posible generación de datos en cuanto a feedback del servicio recibido de cara a facilitar el cumplimiento del SLA contratado con el operador.

Independientemente de las mejoras que proporcionan los avances tecnológicos en cuanto a equipos informáticos de altas prestaciones o el aumento de la capacidad de gestión que incorporan las redes basadas en políticas, hay otros factores también importantes que hacen que el rendimiento de la red sea más óptima. En el caso de este proyecto se ha experimentado con la influencia de varios factores en concreto para evaluar el rendimiento de la arquitectura diseñada y sus posibles mejoras, estos factores son los siguientes: velocidad de señalización de los canales que comunican las entidades (64 Kbps o 2Mbps), tipo de proceso de autenticación utilizado (serie o paralelo) e influencia de estar o no conectado al Home Operator.

Analizando los resultados obtenidos en el capítulo de resultados se puede decir que hay dos factores cruciales en cuanto a mejora de rendimiento de la arquitectura. Por una parte, si nos fijamos en el retardo promedio del servicio de una petición, ya sea de nuevo servicio o de traspaso, el uso de la autenticación en paralelo proporciona una reducción considerable respecto al uso de una autenticación en serie, concretamente de alrededor de un 24 % con enlaces de señalización de 64 Kbps y de alrededor de un 10 % con enlaces de señalización de 2 Mbps. El único pero de esta mejora es la pequeña pérdida de seguridad momentánea debida a la ejecución en paralelo de la autenticación junto con el servicio de la petición, pero la relación rendimiento/seguridad lo justifica.

Por otra parte, el factor más influyente en el rendimiento de la arquitectura es la velocidad de los enlaces de señalización. Centrándonos en la mejora del retardo conseguimos una media de un 77 % de reducción, tanto usando autenticación en paralelo como en serie. Además, mediante las simulaciones realizadas se ha apreciado que la funcionalidad de la arquitectura diseñada mejora con el uso de los enlaces de señalización a 2 Mbps, ya que a 64 Kbps se han apreciado fallos funcionales en el momento de la actualización de la ocupación de recursos que tienen las redes, ya que se produce una desincronización entre la información real y la que recibe la FGT a la hora de ejecutar el algoritmo de selección de celda. Esto provoca que las peticiones de traspaso se vean perjudicadas respecto a las peticiones de nuevo servicio, al contrario de lo que necesitamos, ya que los traspasos deberían tener igual o mayor prioridad que las peticiones de nuevo servicio. Por lo tanto, el aumento de la velocidad de los enlaces de señalización es un factor clave en el buen funcionamiento de la arquitectura.

A modo de resumen, en este Proyecto Final de Carrera se ha presentado:

- Información básica del estado de las redes de telecomunicaciones actuales, partiendo de UMTS como base.

- Conceptos generales en cuanto a los diferentes temas a tener en cuenta para el diseño de la arquitectura de gestión de la tarificación para un entorno de red de telecomunicaciones móviles avanzadas: autenticación, tarificación, PBN, movilidad y traspasos.

- Análisis de los requerimientos generales de la arquitectura y diseño de ésta en función de los requisitos que impongan los escenarios en los cuales deberá estar operativa y los servicios que en ella se implementarán.

- Análisis teórico de los diferentes escenarios posibles y del comportamiento de la arquitectura en cada uno de ellos.

- Diseño del protocolo utilizado en cada una de las configuraciones o casos posibles en el escenario más complejo.

- Análisis teórico, mediante programas de simulación que permiten determinar las prestaciones de la arquitectura según sus parámetros de diseño y el protocolo utilizado.

- Optimizar el modelo de gestión en base a la influencia de la variación de los diferentes parámetros de diseño de la arquitectura o protocolo utilizado (velocidad líneas de transmisión, método de autenticación utilizado) y de la variación de algunos parámetros referentes al escenario (tasa de tráfico entrante, operador al que está conectado inicialmente el usuario y tipo de servicio solicitado).

6 Referencias

[1]. 3GPP TS 23.101 – General Universal Mobile Telecommunications System (UMTS) architecture

[2]. 3GPP TS 33.919 – Generic Authentication architecture (GAA), System description

[3]. 3GPP TS 33.220 – Generic Authentication architecture (GAA), Generic bootstrapping architecture

[4]. 3GPP TS 33.220 – Generic Authentication architecture (GAA), Support for subscriber certificates

[5]. M. Wahl et al. "Lightweight Directory Access Protocol (v3)", RFC 2251, IETF

[6]. D. Durham et al. "The COPS (Common Open Policy Protocol)", RFC 2748, IETF

[7]. C. Rigney et al."Remote Authentication Dial In User Server (RADIUS)", RFC 2865, IETF, June 2000

[8]. C. Rigney et al. "RADIUS Accounting", RFC 2866, IETF, June 2000

[9]. P.Calhoun (Airspace, Inc.), J.Loughney (Nokia) et al. "Diameter Based Protocol", RFC 3588, IETF, September 2003

[10]. Barba Marti A., Guerrero Ibañez J.A., A network selection mechanism for next generation Mobile Communications, 3rd IET International Conference on Intelligent Environments (IE07), September 24-25, 2007

[11]. www.omnetpp.org

Anexo 1

Tablas de resultados

A1.1 AA serie – Nueva celda escogida pertenece al HO – 64 Kbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	298,92	299,07	299,06	299,13	299,55	299,9	300,05	300,14	300,44	301,29
Máximo retardo de traspaso	325,62	325,62	325,62	325,62	325,62	325,62	325,62	325,62	325,62	325,62
Desviación estándar de traspaso	33,21	33,17	33,18	33,16	33,06	32,98	32,94	32,92	32,84	32,6
Retardo promedio de nuevo servicio	228,51	228,74	229,07	229,24	229,5	229,89	230,12	230,29	230,46	231,19
Máximo retardo de nuevo servicio	255,6	255,59	255,59	255,59	255,59	255,59	255,59	255,59	255,59	255,59
Desviación estándar de nuevo servicio	33,29	33,25	33,17	33,13	33,07	32,97	32,91	32,87	32,83	32,62
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,06	2,82	6,65	9,81	12,99	17,63	23,16
De traspaso (%)	0,00	0,00	0,00	0,08	3,66	8,57	12,63	16,94	23,05	29,35
De nuevo servicio (%)	0,00	0,00	0,00	0,04	1,56	3,77	5,52	7,02	9,50	13,93
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	0,07	0,22	0,45	0,89	3,32	7,98
De traspaso (%)	0,00	0,00	0,00	0,00	0,06	0,23	0,45	0,90	3,33	7,97
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,07	0,21	0,46	0,88	3,31	8,00
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,06	2,75	6,45	9,40	12,21	14,80	16,49
De traspaso (%)	0,00	0,00	0,00	0,12	5,36	12,56	18,50	24,27	29,60	31,87
De nuevo servicio (%)	0,00	0,00	0,00	0,04	1,49	3,57	5,09	6,19	6,41	6,44

A1.2 AA paralelo – Nueva celda escogida pertenece al HO – 64 Kbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	227,74	227,83	227,87	227,93	228,28	228,69	229,13	229,36	229,45	229,9
Máximo retardo de traspaso	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13
Desviación estándar de traspaso	33,16	33,18	33,17	33,15	33,08	32,98	32,87	32,8	32,78	32,65
Retardo promedio de nuevo servicio	157,56	157,74	157,67	157,67	158,17	158,54	158,9	158,99	159,28	159,52
Máximo retardo de nuevo servicio	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68
Desviación estándar de nuevo servicio	33,18	33,19	33,16	33,15	33,04	32,95	32,86	32,83	32,75	32,68
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,01	2,59	6,29	10,09	13,41	18,32	23,42
De traspaso (%)	0,00	0,00	0,00	0,02	3,38	8,18	13,05	17,33	22,97	28,20
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,41	3,44	5,66	7,51	11,35	16,22
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	0,28	0,73	1,53	2,75	7,02	12,53
De traspaso (%)	0,00	0,00	0,00	0,00	0,28	0,75	1,55	2,75	7,08	12,58
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,27	0,70	1,50	2,77	6,94	12,46
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,01	2,32	5,61	8,69	10,96	12,15	12,46
De traspaso (%)	0,00	0,00	0,00	0,03	4,63	11,24	17,22	21,97	23,82	23,57
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,14	2,76	4,22	4,88	4,74	4,29

A1.3 AA serie – Nueva celda escogida NO pertenece al HO – 64 Kbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	300,58	300,33	300,56	300,54	300,87	301,39	301,47	301,65	301,78	302,64
Máximo retardo de traspaso	327,07	327,08	327,08	327,07	327,08	327,08	327,08	327,08	327,08	327,08
Desviación estándar de traspaso	33,18	33,24	33,19	33,2	33,13	32,99	32,97	33,93	32,89	32,65
Retardo promedio de nuevo servicio	230,54	230,25	230,36	230,64	231,01	231,09	231,5	231,59	231,95	232,55
Máximo retardo de nuevo servicio	256,98	256,99	256,98	256,99	256,99	256,99	256,99	256,99	256,99	256,98
Desviación estándar de nuevo servicio	33,16	33,22	33,19	33,13	33,04	33,02	32,92	32,89	32,8	32,63
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,01	2,77	6,42	9,85	12,77	17,72	23,12
De traspaso (%)	0,00	0,00	0,00	0,02	3,63	8,27	12,71	16,63	23,00	29,23
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,49	3,65	5,56	6,99	9,77	13,94
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	0,08	0,19	0,46	0,90	3,46	8,10
De traspaso (%)	0,00	0,00	0,00	0,00	0,09	0,19	0,44	0,90	3,45	8,13
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,06	0,17	0,49	0,91	3,48	8,07
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,01	2,69	6,25	9,44	11,97	14,77	16,33
De traspaso (%)	0,00	0,00	0,00	0,02	5,27	12,08	18,38	23,55	29,42	31,67
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,43	3,48	5,10	6,13	6,52	6,39

A1.4 AA paralelo – Nueva celda escogida NO pertenece al HO – 64 Kbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	227,74	227,83	227,87	227,93	228,29	228,47	229,13	229,25	229,45	229,9
Máximo retardo de traspaso	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13	255,13
Desviación estándar de traspaso	33,16	33,17	33,16	33,14	33,07	33,03	32,87	32,83	32,78	32,64
Retardo promedio de nuevo servicio	157,56	157,53	157,67	157,67	158,17	158,68	158,88	159	159,28	159,52
Máximo retardo de nuevo servicio	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68	184,68
Desviación estándar de nuevo servicio	33,18	33,19	33,6	33,15	33,04	32,92	32,87	32,83	32,75	32,68
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,01	2,59	6,24	10,05	13,38	18,32	23,42
De traspaso (%)	0,00	0,00	0,00	0,02	3,38	8,07	12,99	17,22	22,97	28,20
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,41	3,49	5,63	7,61	11,35	16,22
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	0,28	0,77	1,52	2,81	70,2	12,53
De traspaso (%)	0,00	0,00	0,00	0,00	0,28	0,77	1,54	2,78	7,08	12,58
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,27	0,76	1,49	2,84	6,94	12,46
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,01	2,32	5,52	8,66	10,88	12,15	12,46
De traspaso (%)	0,00	0,00	0,00	0,03	4,63	11,03	17,17	21,73	23,82	23,57
De nuevo servicio (%)	0,00	0,00	0,00	0,01	1,14	2,75	4,20	4,91	4,74	4,29

A1.5 AA serie – Nueva celda escogida pertenece al HO – 2 Mbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	60,82	60,83	60,83	60,83	60,84	60,84	60,86	60,86	60,85	60,85
Máximo retardo de traspaso	61,62	61,62	61,62	61,62	61,63	61,63	61,63	61,63	61,62	61,62
Desviación estándar de traspaso	0,98	0,98	0,98	0,98	0,98	0,98	0,97	0,97	0,98	0,98
Retardo promedio de nuevo servicio	56,8	56,79	56,8	56,8	56,81	56,82	56,83	56,83	56,83	56,83
Máximo retardo de nuevo servicio	57,59	57,59	57,59	57,6	57,6	57,6	57,6	57,6	57,6	57,6
Desviación estándar de nuevo servicio	0,98	0,99	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,00	2,45	7,25	11,59	15,68	21,13	25,37
De traspaso (%)	0,00	0,00	0,00	0,00	2,43	7,27	11,67	15,67	21,11	25,39
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,48	7,22	11,47	15,71	21,16	25,38
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	2,40	7,06	11,30	15,51	21,07	25,33
De traspaso (%)	0,00	0,00	0,00	0,00	2,37	7,07	11,41	15,49	21,05	25,32
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,43	7,04	11,15	15,53	21,10	25,34
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,00	0,05	0,20	0,32	0,21	0,08	0,05
De traspaso (%)	0,00	0,00	0,00	0,00	0,08	0,29	0,39	0,28	0,09	0,06
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,05	0,19	0,36	0,20	0,08	0,06

A1.6 AA paralelo – Nueva celda escogida pertenece al HO – 2 Mbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	55,27	55,27	55,27	55,27	55,28	55,29	55,3	55,29	55,29	55,29
Máximo retardo de traspaso	56,06	56,06	56,06	56,06	56,06	56,06	56,06	56,06	56,07	56,07
Desviación estándar de traspaso	0,98	0,98	0,98	0,98	0,98	0,98	0,97	0,98	0,98	0,98
Retardo promedio de nuevo servicio	51,24	51,24	51,24	51,24	51,24	51,26	51,27	51,27	51,27	51,27
Máximo retardo de nuevo servicio	52,04	52,04	52,04	52,03	52,04	52,03	52,04	52,04	52,04	52,04
Desviación estándar de nuevo servicio	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,00	2,18	7,14	11,36	15,49	20,97	25,10
De traspaso (%)	0,00	0,00	0,00	0,00	2,20	7,19	11,42	15,59	21,01	25,06
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,14	7,06	11,26	15,35	20,91	25,16
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	2,13	6,97	11,11	15,26	20,89	25,07
De traspaso (%)	0,00	0,00	0,00	0,00	2,16	7,01	11,18	15,36	20,93	25,03
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,10	6,91	11,00	15,12	20,83	25,13
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,00	0,04	0,18	0,28	0,27	0,10	0,04
De traspaso (%)	0,00	0,00	0,00	0,00	0,06	0,26	0,37	0,34	0,11	0,04
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,05	0,17	0,29	0,27	0,10	0,04

A1.7 AA serie – Nueva celda escogida NO pertenece al HO – 2 Mbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	62,21	62,21	62,22	62,22	62,23	62,24	62,25	62,25	62,25	62,24
Máximo retardo de traspaso	63	63,01	63	63,01	63,01	63,01	63	63,01	63,01	63
Desviación estándar de traspaso	0,98	0,98	0,98	0,98	0,98	0,98	0,97	0,97	0,97	0,98
Retardo promedio de nuevo servicio	58,19	58,19	58,19	58,19	58,2	58,21	58,22	58,22	58,22	58,22
Máximo retardo de nuevo servicio	58,98	58,98	58,98	58,98	58,99	58,99	58,99	58,99	58,99	58,99
Desviación estándar de nuevo servicio	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,00	2,60	7,25	11,34	15,70	20,96	25,44
De traspaso (%)	0,00	0,00	0,00	0,00	2,65	7,24	11,40	15,63	20,82	25,42
De nuevo servicio (%)	0,00	0,00	0,00	0,01	2,53	7,27	11,26	15,79	21,18	25,48
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	2,56	7,08	11,10	15,50	20,90	25,41
De traspaso (%)	0,00	0,00	0,00	0,00	2,61	7,07	11,16	15,45	20,76	25,39
De nuevo servicio (%)	0,00	0,00	0,00	0,01	2,49	7,09	11,02	15,58	21,10	25,44
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,00	0,04	0,18	0,27	0,23	0,08	0,05
De traspaso (%)	0,00	0,00	0,00	0,00	0,06	0,24	0,36	0,28	0,09	0,05
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,04	0,20	0,27	0,25	0,09	0,05

A1.8 AA paralelo – Nueva celda escogida NO pertenece al HO – 2 Mbps

Peticiones por ráfaga	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**
Retardo promedio de traspaso	55,27	55,27	55,27	55,27	55,28	55,29	55,3	55,3	55,3	55,3
Máximo retardo de traspaso	56,06	56,06	56,06	56,06	56,06	56,06	56,06	56,06	56,06	56,07
Desviación estándar de traspaso	0,98	0,98	0,98	0,98	0,97	0,97	0,97	0,97	0,97	0,97
Retardo promedio de nuevo servicio	51,24	51,24	51,24	51,24	51,24	51,26	51,27	51,27	51,27	51,27
Máximo retardo de nuevo servicio	52,04	52,03	52,04	52,04	52,04	52,04	52,04	52,04	52,04	52,04
Desviación estándar de nuevo servicio	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98	0,98
Peticiones totales rechazadas (%)	0,00	0,00	0,00	0,00	2,18	7,14	11,36	15,62	20,97	25,10
De traspaso (%)	0,00	0,00	0,00	0,00	2,20	7,19	11,42	15,64	21,01	25,06
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,14	7,06	11,26	15,59	20,91	25,16
Peticiones rechazadas en la FGT (%)	0,00	0,00	0,00	0,00	2,13	6,97	11,11	15,42	20,89	25,07
De traspaso (%)	0,00	0,00	0,00	0,00	2,16	7,01	11,18	15,44	20,93	25,03
De nuevo servicio (%)	0,00	0,00	0,00	0,00	2,10	6,91	11,00	15,39	20,83	25,13
Peticiones rechazadas en Esx (%)	0,00	0,00	0,00	0,00	0,04	0,18	0,28	0,24	0,10	0,04
De traspaso (%)	0,00	0,00	0,00	0,00	0,06	0,26	0,37	0,30	0,11	0,04
De nuevo servicio (%)	0,00	0,00	0,00	0,00	0,05	0,17	0,29	0,24	0,10	0,04

Anexo 2

Estimación de retardos

Para la evaluación del protocolo, necesitamos especificar los distintos retardos producidos por los diferentes elementos y transmisiones que intervienen en la comunicación. Para ello, inicialmente debemos justificar los retardos considerados y los parámetros de los cuáles dependen. En este apartado se describen las características de los diferentes elementos que introducen retardo en el protocolo.

A2.1 Radioenlace

Seguramente, el elemento más crítico en la evaluación del protocolo, ya que es el que introduce más retardo en la comunicación. Los parámetros que se considerarán para establecer el retardo son los siguientes:

3 Tecnología utilizada (UMTS, WiFi, ...)
4 Procedimiento de acceso aleatorio
5 Radio de la celda
6 Estructura y duración de trama
7 Tasa de transmisión de información
8 Probabilidad de error

Dado que cada tecnología viene marcada por diferentes características, como por ejemplo, tasa de transmisión, estructura de trama, procedimiento de acceso, probabilidad de error, alcance máximo, etc., el retardo final asociado al radio enlaces variará sustancialmente al considerar una tecnología u otra.

A2.1.1 UMTS

Las características más relevantes del interfaz radio UMTS (UTRA) son las siguientes:

Esquema de acceso múltiple	DS – CDMA
Esquema de duplexado	FDD / TDD
Velocidad de chip	3,84 Mcps
Ancho de banda por canal radio	5 MHz
Duración de trama	10 ms
Tasa de transmisión de información	Variable según el factor de ensanchamiento en espectro
Esquema de codificación de canal	Codificación convolucional y turbo códigos
Probabilidad de error	VER de 10^{-4}

A partir de estas características y del estudio del procedimiento de acceso aleatorio, determinaremos la expresión del retardo del radio enlaces en función de varios de los parámetros anteriormente mencionados.

Procedimiento de acceso aleatorio

Cuando un terminal móvil pretende acceder al sistema lo hace a través del canal de acceso aleatorio RACH. El terminal móvil decodifica el canal BCCH para identificar los subcanales RACH disponibles para esa estación base. Dicho terminal móvil escoge un subcanal RACH e inicia la emisión del primer preámbulo, tal y como se representa en la Figura 1, con un nivel de potencia inicial estimado según el algoritmo de control de potencia en bucle abierto. A partir de ese momento emite sucesivos preámbulos con un nivel de potencia creciente hasta recibir contestación por el canal AICH. A continuación el terminal móvil emite el correspondiente mensaje de longitud equivalente a una o dos tramas (10 o 20 ms).

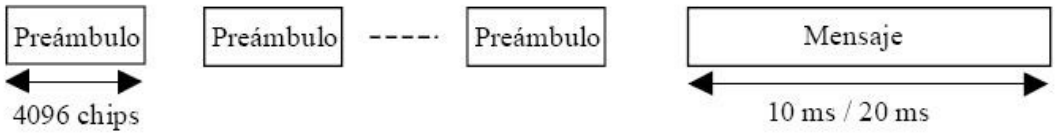


Figura 1. Estructura de trama del canal de acceso aleatorio

Por su parte, la estación base cuenta con un correlador adaptado al código del preámbulo utilizado por dicha estación base. El código de preámbulo utilizado es indicado por la estación base a través del canal BCCH. A la salida del correlador se obtendrá un pico de señal correspondiente al instante en que se recibe la ráfaga de acceso, lo cuál será indicativo del intento de acceso por parte de un terminal móvil.

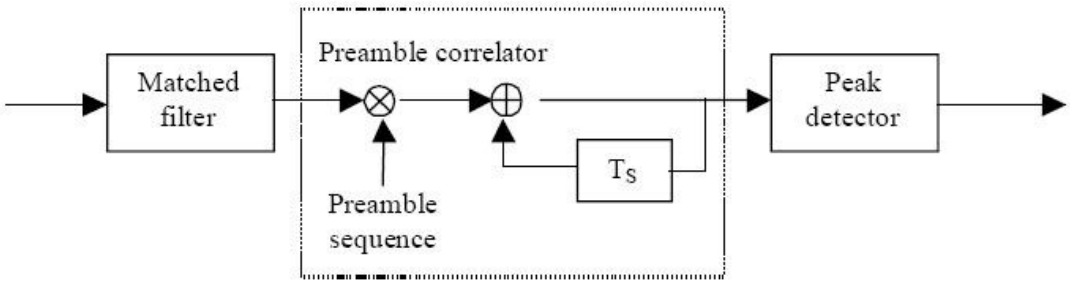


Figura 2. Receptor de acceso aleatorio de la estación base

El canal AICH (Acquisition Indication Channel) transporta las respuestas a los preámbulos de acceso al canal PRACH. El AICH consta de 15 intervalos de acceso equivalentes a dos radio normales, aunque sólo se utilizan los primeros 4.096 chips para la emisión de 32 bits de información, lo mismo que sucede con los preámbulos del canal PRACH. Véase la Figura 3.

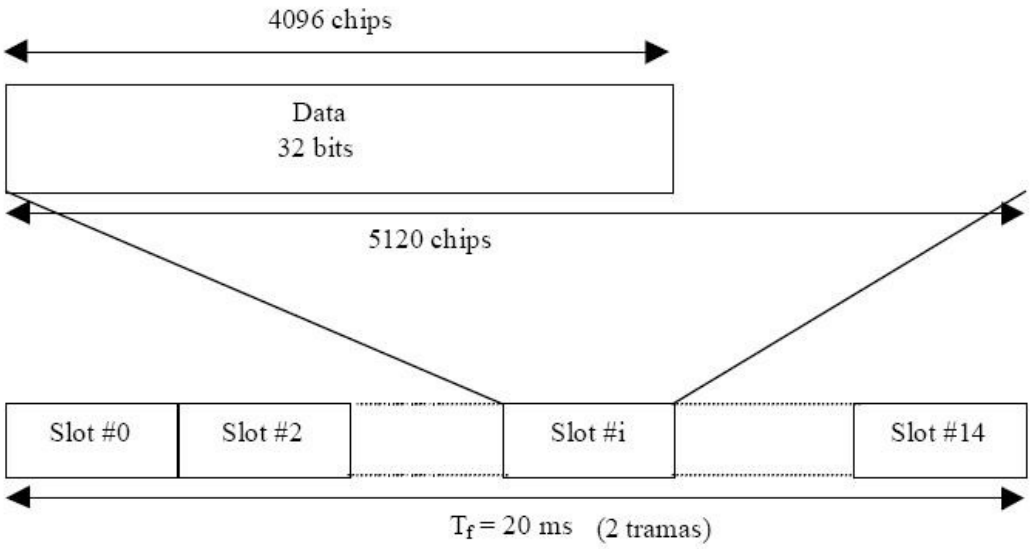


Figura 3. Estructura de trama del canal AICH

Cálculo del retardo

Después de haber presentado el procedimiento de acceso aleatorio, nos queda obtener una expresión que nos dé una idea de cómo influye cada parámetro en el retardo. Para ello debemos separar el procedimiento en distintas fases:

8.1 Envío del preámbulo
8.2 Evaluación del intento de acceso por la estación base
8.3 Contestación por el canal AICH
8.4 Emisión de un mensaje por parte del terminal móvil

→ Envío del preámbulo

El preámbulo tiene una duración de 4096 chips, se envía uno cada 5120 chips hasta recibir confirmación y la velocidad de chip es de 3,84 Mcps.

Tiempo de transmisión de un preámbulo = Tpre = $\frac{4096}{3{,}84 \cdot 10^6}$ = 1,07 ms

Tiempo de 2 slots = T2slots = $\frac{5120}{3{,}84 \cdot 10^6}$ = 1,33 ms

→ Evaluación del intento de acceso por la estación base

En caso de que la potencia de la señal enviada no sea la suficiente o los canales estén ocupados el terminal móvil deberá esperarse para el acceso. Por lo tanto, el terminal móvil continuará enviando preámbulos hasta ser aceptada su petición de acceso.

Tiempo de aceptación = Tacep = $1{,}07 \cdot N + 1{,}33 \cdot (N-1)$ [ms] ; N >0

Donde N es el número de intentos necesarios para que la estación base acepte nuestra petición de acceso.

→ Contestación por el canal AICH

Una vez aceptada la petición de acceso, se envían 4096 chips de información por el canal AICH cada 5120 chips, tal y como se apreciaba en la Figura 3.

$$\text{Tiempo de contestación} = \text{Tcon} = \frac{4096}{3{,}84 \cdot 10^6} = 1{,}07 \text{ ms}$$

→ Emisión de un mensaje por parte del terminal móvil

Una vez recibida la información por el canal AICH, el terminal móvil emite una mensaje propio sobre el canal PRACH, cuya duración oscila entre una y dos tramas (10 – 20 ms).

Tmen = 10 – 20 ms

NOTA: El tiempo de propagación necesario para que la información llegue desde el terminal móvil a la estación base y viceversa ha sido despreciado en comparación con los tiempos necesarios para el envío de preámbulos y mensajes, ya que, como máximo, con una celda de radio 10 Km., el tiempo de propagación seria:

$$\text{Tprop} = \frac{10.000}{3 \cdot 10^8} = 33\mu s$$ → poco más de un 3% de la transmisión de un preámbulo.

Por lo tanto, el retardo total necesario para obtener el acceso a la red es el resultado de la siguiente fórmula:

$$\text{Tacc} = 1{,}07 \cdot N + 1{,}33 \cdot (N - 1) + 1{,}07 + 20 \text{ [ms]} = 2{,}40 \cdot N + 19{,}74 \text{ [ms]}$$

Hemos considerado que se envía un mensaje de dos tramas de duración, para obtener el límite superior del retardo.

→ Probabilidad de error

A continuación, para que el tiempo de acceso sea más riguroso, tendremos en cuenta la influencia de una probabilidad de error en la transmisión del mensaje.

Consideramos que el tiempo que se tarda en la detección de un error en el mensaje y el inicio de la retransmisión es el correspondiente a la transmisión de un preámbulo, es decir, 1,07 ms, considerando un tiempo de proceso despreciable por parte de la estación base.

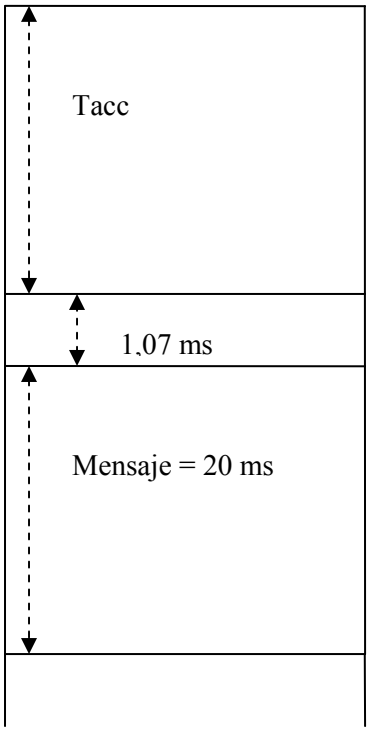


Figura 4. Esquema de retransmisiones en caso de error

El tiempo medio de transmisión, con probabilidad de error, vendrá dado por la siguiente fórmula:

$$\overline{T} = Tacc \cdot q + Tacc \cdot p \cdot q + Tret \cdot p \cdot q + Tacc \cdot p^2 \cdot q + Tret \cdot p^2 \cdot q + Tacc \cdot p^3 \cdot q + Tret \cdot p^3 \cdot q + ... =$$

$$= q \cdot Tacc \cdot \sum_{n=0}^{\infty} p^n + q \cdot Tret \cdot \sum_{n=0}^{\infty} n \cdot p^n = Tacc + Tret \cdot \frac{p}{q} = Tacc + Tret \cdot \frac{p}{1-p}$$

Donde p es la probabilidad de error del mensaje, calculada de la siguiente forma:

Duración mensaje = 20 ms → 600 bits → $p = 1 - (1 - BER)^{600}$

En nuestro caso el VER es 10^{-4}, por lo tanto, p = 0,0582 y q = 1 – p = 0,9417.

En conclusión, el retardo total acumulado en el radio enlaces, teniendo en cuenta el número de intentos para ser aceptada nuestra petición de acceso, así como, la probabilidad de error en el medio, es el siguiente:

$$\overline{T}_{RAD\_UMTS} = 2{,}40 \cdot N + 19{,}74 + 21{,}07 \cdot \frac{1-(1-BER)^{600}}{(1-BER)^{600}} = 2{,}40 \cdot N + \frac{21{,}07}{(1-BER)^{600}} - 1{,}33 \text{ [ms]}$$

A2.2 Elementos intermedios

A parte del radio enlaces, también habrá otros elementos que influirán en el retardo total del protocolo, aunque seguramente no de forma tan crítica. A continuación pasaremos a describir cada uno de los elementos que aportan retardo extra al sistema y evaluaremos los parámetros que influyen en él.

A2.2.1 Elemento de servicio (ES) y sonda de medición (SM)

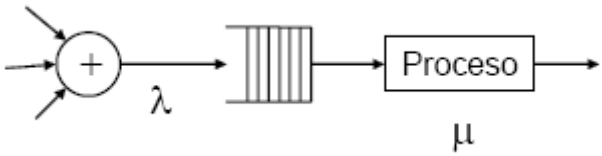
El ES y la SM los hemos modelado como tarjetas de red con una capacidad de proceso de entre 10 – 1000 Mbps las cuáles se comunican con los demás elementos del mismo operador o VASP mediante el estándar Ethernet o similar, en el caso de que estén conectados al mismo equipo (PC) o mediante el canal de señalización SS7, si no están conectados al mismo equipo (PC).

Cálculo del retardo

El retardo asociado a este elemento lo denominaremos t_{ESM} y contemplará el tiempo empleado para las siguientes funciones:

- Procesado y creación de mensajes.
- Establecer una configuración determinada.
- Responder a una petición de datos.

Para obtener los valores máximos y mínimos del retardo usaremos un modelo de colas M/M/1:



La capacidad de proceso estaría entre 10 – 1000 Mbps propia de los modelos de tarjetas de red actuales que trabajan con el estándar Ethernet. Para realizar el cálculo he asumido que los paquetes tendrían un tamaño de entre 50 – 1500 bytes. De modo aproximado, los retardos serían los siguientes:

$$t_{ESM}\ \max = \frac{tamaño\_paquete\_máximo}{capacidad\_de\_proceso\_mínima} = \frac{1500 \cdot 8}{10 \cdot 10^6} = 1{,}2\ \text{ms}$$

$$t_{ESM}\ \min = \frac{tamaño\_paquete\_mínimo}{capacidad\_de\_proceso\_máxima} = \frac{50 \cdot 8}{1000 \cdot 10^6} = 0{,}4\ \mu s$$

Finalmente obtenemos que: $0{,}4\ \mu s < t_{ESM} < 1{,}2\ \text{ms}$

A2.2.2 Función de gestión de la tarificación (FGT)

Este modelo lo considero como un equipo con un procesador robusto que es capaz de trabajar con un reloj de entre 100 – 500 MHz. Para determinar el retardo total en el procesado y creación de mensajes, así como en la creación de AIDs, UIDs y SIDs, me he basado en una aproximación de las instrucciones máquina y ciclos de reloj teóricos que emplea un procesador 486 al realizar accesos a memoria, accesos a registros, cálculos de dirección de memoria efectiva, sumas, restas, multiplicaciones, divisiones, operaciones lógicas, etc.

Cálculo del retardo

El retardo asociado a este elemento lo denominaremos t_{FGT} y contemplará el tiempo empleado para las siguientes funciones:

- Procesado y creación de mensajes.
- Creación de AIDs
- Creación de UIDs
- Creación de SIDs

Para obtener los valores máximos y mínimos del retardo he considerado, de modo aproximado, que se necesitaban 1.000 ciclos de reloj para realizar las distintas operaciones. Para realizar los cálculos he considerado que el procesador podía trabajar con un reloj de entre 100 – 500 MHz. De modo aproximado los retardos serían los siguientes:

$$t_{FGT}\,\max = \frac{ciclos\_de\_reloj\_empleados}{velocidad\_del\_procesador\_mínima} = \frac{1000}{100 \cdot 10^6} = 10\ \mu s$$

$$t_{FGT}\,\min = \frac{ciclos\_de\_reloj\_empleados}{velocidad\_del\_procesador\_máxima} = \frac{1000}{500 \cdot 10^6} = 2\ \mu s$$

Finalmente obtenemos que: $\boxed{2\ \mu s < t_{FGT} < 10\ \mu s}$

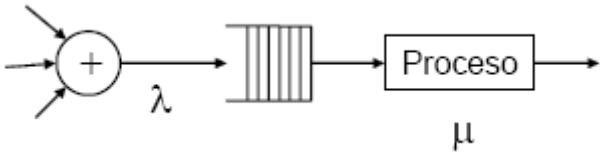
A2.2.3 Nodos intermedios

Para la comunicación entre operadores y entre operadores y VASP he considerado que hay nodos intermedios los cuales procesan la información y la transmiten hasta el siguiente nodo antes de llegar al operador o VASP final. Estos nodos también introducen retardo en la comunicación, ya que deben desencapsular y volver a encapsular los paquetes, por lo tanto, cuánto mayor sea la distancia entre operadores y VASP, mayor número de nodos intermedios habrán y mayor retardo introducido tendremos. El modelo utilizado es un switch con una capacidad de proceso de entre 10 – 1000 Mbps.

Cálculo del retardo

El retardo asociado a este elemento lo denominaremos t_{NI} y hace referencia al tiempo de procesado empleado por los nodos intermedios entre operadores o entre operadores y VASPs.

Para obtener los valores máximos y mínimos del retardo he usado un modelo de colas M/D/1, ya que el tamaño del paquete acostumbrará a ser siempre igual:



La capacidad de proceso sería de entre 10 – 1000 Mbps. La probabilidad de que el sistema este ocupado sería $\rho = 0.5$. Además, para realizar el cálculo he asumido que los paquetes tendrían un tamaño de entre 50 – 1500 bytes. De modo aproximado, los retardos serían los siguientes:

Número promedio de unidades que se encuentran en el sistema, ya sea esperando o siendo atendidas:

$$L = \frac{\rho \cdot (2-\rho)}{2 \cdot (1-\rho)} = \frac{0.5 \cdot (1.5)}{2 \cdot (0.5)} = 0.75$$

Tiempo promedio de una unidad en el sistema: $W = \frac{L}{\lambda} = \frac{L}{\rho \cdot \mu}$

$$t_{NI}\ \max = \frac{L}{\rho \cdot \mu \min} = \frac{0.75}{0.5 \cdot \frac{10 \cdot 10^6}{1500 \cdot 8}} = 1{,}8 \text{ ms}$$

$$t_{NI}\ \min = \frac{L}{\rho \cdot \mu \max} = \frac{0.75}{0.5 \cdot \frac{1000 \cdot 10^6}{50 \cdot 8}} = 0.6\ \mu s$$

Finalmente obtenemos que: $0{,}6\ \mu s < t_{NI} < 1{,}8$ ms

A2.2.4 Servidores AA

El modelo utilizado es un ordenador (PC) cuyo tiempo empleado para los cálculos se considera como una parámetro variable y del cuál no obtendremos valores aproximados, simplemente estableceremos los márgenes por los cuáles debería moverse para que los diferentes protocolos funcionen correctamente.

Cálculo del retardo

El retardo asociado a este elemento lo denominaremos t_{AA} y contemplará el tiempo empleado para las siguientes funciones:

- Leer la información referente a políticas y perfil de usuario.
- Cálculos necesarios para autorizar o no a un usuario para el uso de los servicios.
- Procesado y generación de mensajes.

Tal y como hemos comentado al principio, t_{AA} será una variable independiente la cuál manipularemos para evaluar cómo afecta al funcionamiento del protocolo.

t_{AA} variable

A2.2.5 Contenedores de información (CT)

El modelo utilizado es el de un disco duro. Los retardos que consideraremos serán los debidos al tiempo medio de búsqueda en la lectura y la escritura. Además se considerará también el tiempo empleado para la transferencia de los datos en la lectura o escritura de ficheros. Los valores utilizados provienen de los datasheets de productos comerciales de Maxtor, Seagate y Western Digital. Utilizaremos una latencia promedio de 3 ms y una tasa de transferencia de 1.5 Gb/s. A parte, también añadiremos como retardo el tiempo empleado para transmitir los datos desde el disco duro hasta la tarjeta de red, para ello usaremos los datos referentes a las tasas de transferencia de los buses VME, concretamente de 20 Mbyte/s. Cabe destacar que el proceso de escritura se diferencia del de lectura porque en el primero se deberá verificar que lo que se escribe es correcto, por lo tanto, tendremos un retardo adicional que llamaremos t_V y que por el momento no asignaremos un valor concreto.

Cálculo del retardo de lectura

El retardo asociado a este elemento lo denominaremos t_{CTL} y hace referencia al tiempo empleado por el contenedor de información de tarificación (CT) para leer información referente a perfiles de usuario, políticas, etc.

Suponiendo que los ficheros a leer tienen un tamaño de 1 – 10 Kbytes:

$$t_{CL}\,\max = 3\,\text{ms} + \frac{10.000 \cdot 8}{1.5 \cdot 10^9} + \frac{10.000}{20 \cdot 10^6} = 3.55\ \text{ms}$$

$$t_{CL}\,\min = 3\,\text{ms} + \frac{1.000 \cdot 8}{1.5 \cdot 10^9} + \frac{1.000}{20 \cdot 10^6} = 3.06\ \text{ms}$$

Finalmente obtenemos que:

3,06 ms < t_{CTL} < 3,55 ms

Cálculo del retardo de escritura

El retardo asociado a este elemento lo denominaremos t_{CTE} y hace referencia al tiempo empleado por el contenedor de información de tarificación (CT) para escribir la información referente a perfiles de usuario, políticas, etc. Contempla las siguientes funciones:

- Escritura de perfiles de usuario, políticas, etc.
- Verificar la correcta sintaxis.
- Rectificar los errores de sintaxis en caso necesario.

El tiempo empleado para la escritura será el mismo que para la lectura más un tiempo adicional correspondiente a la verificación y rectificación si es necesario de errores en la sintaxis.

Finalmente obtenemos que: $3{,}06 \text{ ms} + t_V < t_{CTE} < 3{,}55 \text{ ms} + t_V$

A2.2.6 Terminal de usuario (TU)

Teniendo en cuenta la evolución que están teniendo los teléfonos móviles en cuanto a prestaciones y capacidad de proceso, se considera que el tiempo empleado para asimilar los mensajes recibidos y actuar en consecuencia es prácticamente despreciable en comparación a los demás retardos considerados en el escenario. Pero lo que si deberemos de tener en cuenta será el tiempo empleado por el algoritmo de selección de celda.

Cálculo del retardo

El retardo asociado a este elemento lo denominaremos t_{TU} y hará referencia al tiempo requerido por el algoritmo de selección de celda.

Este tiempo será una variable independiente que manipularemos para evaluar cómo afectan los diferentes valores al funcionamiento del protocolo.

t_{TU} variable

A2.3 Propagación y transmisión

A parte de los retardos introducidos por los elementos que procesan la información, también tenemos otros retardos debidos al tiempo que tarda la información en llegar a los diferentes elementos funcionales, ya sea mediante ondas radioeléctricas o a través de su transmisión por cable o fibra óptica de diferentes velocidades de transmisión y propagación.

Dentro de los retardos asociados a la transmisión diferenciamos dos tipos de retardos, el retardo de propagación y el retardo de transmisión.

A2.3.1 Retardo de propagación

Este retardo es debido al tiempo que necesita la señal para propagarse por los distintos medios de transmisión. Este retardo dependerá del medio por el cual se propague (aire, cobre, fibra óptica, etc.) y de la distancia que debe recorrer la señal.

El retardo de propagación lo denominaremos t_P, y el cálculo de su valor lo realizaremos con la siguiente fórmula:

$$t_P = \frac{D}{NVP \cdot C}$$

Donde:

- C = 300.000 Km/s es la velocidad de la luz en el vacío.
- D es la distancia que separa a los nodos por los cuales se transmitirá la información.
- NVP = Velocidad Nominal de Propagación (en %)

Cálculo del retardo

A la hora de calcular los retardos, debemos diferenciar dos medios de transmisión: transmisión por el aire y transmisión por cable.

→ ***Transmisión por aire***

En la transmisión por aire, tenemos que la NVP = 100 %. Los retardos más comunes serían los siguientes:

- Pico celda (D = 20 m) $\Rightarrow$ $t_P \approx$ 70 ns
- Micro celda (D = 200 m) $\Rightarrow$ $t_P \approx$ 700 ns
- Macrocelda (D = 10 Km) $\Rightarrow$ $t_P \approx 35\ \mu s$
- Satélites MEO (D = 10.000 Km) $\Rightarrow$ $t_P \approx$ 33 ms
- Satélites GEO (D = 35.800 Km) $\Rightarrow$ $t_P \approx$ 119 ms

→ ***Transmisión por cable***

En la transmisión por cable, tenemos que la NVP = 67 %. Los retardos más comunes serían los siguientes:

- Transmisión en una misma calle (D = 100 m) $\Rightarrow$ $t_P \approx$ 500 ns
- Transmisión entre barrios contiguos (D = 1 Km) $\Rightarrow$ $t_P \approx 5\ \mu s$
- Transmisión entre barrios no contiguos (D = 10 Km) $\Rightarrow$ $t_P \approx 50\ \mu s$
- Transmisión Barcelona – Girona (D = 100 Km) $\Rightarrow$ $t_P \approx 500\ \mu s$
- Transmisión Barcelona – Málaga (D = 1.000 Km) $\Rightarrow$ $t_P \approx$ 5 ms
- Transmisión Barcelona – Shangai (D = 10.000 Km) $\Rightarrow$ $t_P \approx$ 50 ms

A2.3.2 Retardo de transmisión

Este retardo es debido al tiempo que se necesita para que el último bit del mensaje haya sido enviado al siguiente elemento funcional. Este retardo dependerá básicamente del

tamaño del mensaje o paquete y de la velocidad de transmisión de la línea por la cuál se transmite.

El retardo de transmisión lo denominaremos t_{TX}, y el cálculo de su valor lo realizaremos con la siguiente fórmula:

$$t_{TX} = \frac{L}{R}$$

Donde:

- L es el tamaño en bits de los mensajes o paquetes enviados. El tamaño puede variar entre 50 – 1500 bytes dependiendo del tipo de mensaje o paquete enviado.
- R es la velocidad de la transmisión. Para el canal radioeléctrico tomaremos unas velocidades de transmisión entre 64 – 2048 Kbps dependiendo la tecnología utilizada (WiFi, UMTS, GSM, etc.). Para la señalización entre nodos tomaremos la velocidad de 64 Kbps que utiliza el protocolo SS7.

Dentro de los retardos de transmisión podemos diferenciar dos tipos, los producidos en el canal radioeléctrico y los producidos en la señalización entre nodos.

→ ***Canal radioeléctrico***

En las transmisiones por canal radioeléctrico nos moveremos entre unas velocidades de 64 – 2048 Kbps, y con unos tamaños de paquetes de entre 50 – 1500 bytes, así que el retardo se moverá entre los siguientes valores:

- Máximo (R = 64 Kbps, L = 1500 bytes): $t_{TX}\,\max = \frac{1500 \cdot 8}{64.000} = 187.5$ ms
- Mínimo (R = 2048 Kbps, L = 50 bytes):

$$t_{TX}\,\min = \frac{50 \cdot 8}{2.048.000} = 195\ \mu s$$

Finalmente tendremos que: $0{,}195 \text{ ms} < t_{TX} < 187{,}5 \text{ ms}$

→ ***Señalización entre nodos***

El campo de información de la señalización consiste en un número entero de bytes y contiene como mínimo los siguientes campos: etiqueta de encaminamiento (4 bytes), tipo de mensaje (1 byte), clase de protocolo (1 byte), contador de saltos (1 byte), punteros (4 bytes), dirección llamada mínima (3 bytes), dirección llamante mínima (2 bytes) y el campo de longitud del parámetro de datos (1 byte). Por lo tanto, el mensaje de menor longitud consta de 17 bytes. Además, como cota superior, de acuerdo con la recomendación UIT-T Q.704, la MTP (Message Transfer Part) soporta una longitud máxima de campo de información de señalización sin segmentar de 272 bytes, es decir, el mensaje más largo será de 272 bytes.

NOTA: Cuando la SCCP (Signalling Connection Control Part) es mejorada con capacidades de banda ancha (ediciones 1996 y 2001), puede transportar hasta 4065 bytes de datos de usuario por facilidades MTP-3b (Rec. UIT-T Q.2210) sin segmentación, en un mensaje LUDT (Long Unit Data Message). Sin embargo, no todas las partes de una red tienen que proporcionar facilidades MTP-3b, por eso no lo hemos tenido en cuenta.

El sistema de señalización está optimizado para funcionar en canales digitales de 64 Kbps. También es adecuado para el funcionamiento a velocidades más bajas pero para nuestro estudio consideraremos siempre canales de 64 Kbps.

NOTA: Actualmente hay enlaces de señalización que soportan velocidades de datos de 1,5 a 2 Mbps, pero debido a su escasa implantación no los tendremos en cuenta.

Así que el retardo se moverá entre los siguientes valores:

- Máximo (R = 64 Kbps, L = 272 bytes): $t_{TX}\ \max = \frac{272 \cdot 8}{64.000} = 34\ \text{ms}$
- Mínimo (R = 64 Kbps, L = 17 bytes): $t_{TX}\ \min = \frac{17 \cdot 8}{64.000} \approx 2\,\text{ms}$

Finalmente tendremos que: $2\ \text{ms} < t_{TX} < 34\ \text{ms}$

Como se puede apreciar en los valores calculados, la velocidad de transmisión de las diferentes fases de la comunicación influirá de manera considerable en la elección del protocolo óptimo a utilizar.

Anexo 3

OMNeT++

OMNeT++ es el programa de simulación utilizado para la evaluación del rendimiento de la arquitectura diseñada. Se puede descargar gratuitamente para usos académicos y sin ánimo de lucro en [11]. Además en el enlace proporcionado anteriormente también se podrá encontrar multitud de información acerca de su funcionamiento y documentación sobre pautas y ejemplos de diseño.

A3.1 ¿Qué es OMNet++?

OMNeT++ es un simulador de eventos discretos de red modular orientado a objetos. El simulador puede ser utilizado para:

- modelado de tráfico de redes de telecomunicaciones
- modelado de protocolos
- modelado de redes de colas
- modelado de multiprocesadores y otros sistemas distribuidos de hardware
- validación de arquitecturas hardware
- evaluación de aspectos de rendimiento de sistemas complejos de software
- … modelado de cualquier otro sistema donde la aproximación de eventos discretos sea apropiada.

Un modelo OMNeT++ se compone de módulos anidados jerárquicamente. La profundidad del anidado de módulos no está limitada, lo cual permite al usuario reflejar la estructura lógica del sistema actual en la estructura del modelo. Los módulos se comunican mediante el paso de mensajes. Los mensajes pueden contener estructuras complejas de datos. Los módulos pueden enviar mensajes bien directamente a su destino o bien por una ruta definida, a través de puertas y conexiones.

Los módulos pueden tener sus propios parámetros. Los parámetros pueden ser usados para personalizar el comportamiento del módulo y parametrizar la topología del modelo.

Los módulos en el nivel más bajo de la jerarquía de módulos incluyen el comportamiento. Estos módulos se denominan módulos simples, y son programados en C++ usando la librería de simulación.

Las simulaciones OMNeT++ pueden presentar variaciones en el interfaz de usuario para diferentes propósitos: debugging, demostración y ejecución por lotes. Las interfaces avanzadas de usuario hacen que el interior del modelo sea visible al usuario, permiten el control sobre la ejecución de la simulación e intervenir cambiando variables y/o objetos dentro del modelo. Esto es muy útil en la fase de desarrollo y debbuging del proyecto de simulación. Las interfaces de usuario también facilitan la demostración de cómo trabaja el modelo.

El simulador, así como los interfaces de usuario y las herramientas son transportables: son conocidas para trabajar en Windows y en varias distribuciones de Unix, usando varios compiladores C++.

OMNeT++ también soporta simulaciones paralelas distribuidas. OMNeT++ puede usar varios mecanismos para comunicaciones entre particiones de una simulación paralela distribuida, por con "pipes". El algoritmo de simulación paralela puede ser fácilmente extendido o conectar nuevos. Los modelos no necesitan ninguna instrumentación especial para funcionar en paralelo – es sólo un asunto de configuración.

OMNeT++ puede ser usado incluso para presentaciones en clase de algoritmos de simulación en paralelo, porque las simulaciones pueden funcionar incluso bajo una GUI que proporcione "feedback" detallado sobre que está pasando.

A3.2 Conceptos de modelado

OMNET ++ proporciona al usuario herramientas eficientes para describir la estructura del sistema actual. Algunas de las características principales son:

- Los módulos jerárquicamente anidados
- Los módulos son instancias de tipos de módulos
- Los módulos se comunican con mensaje a través de canales
- Parámetros flexibles del módulo
- Lenguaje de descripción topológica

A3.2.1 Módulos jerárquicos

Un modelo OMNeT++ consiste de módulos anidados jerárquicamente, los cuales se comunican mediante el paso de mensajes entre ellos. A menudo, los modelos en OMNeT++ son mencionados como *redes*. El módulo de nivel más alto es el módulo sistema. El módulo sistema contiene submódulos, los cuales pueden también contener submódulos (Fig. A3.1). La profundidad del anidado del módulo no está limitada; esto permite al usuario reflejar la estructura lógica del sistema actual en la estructura del modelo.

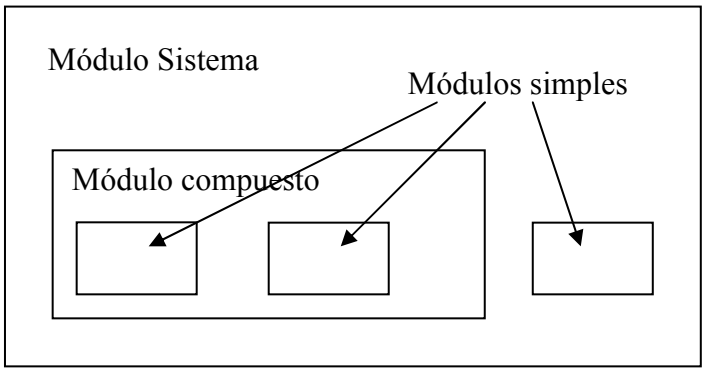


Figura A3.1 –Módulos simples y compuestos

La estructura del modelo es descrita en el lenguaje NED del OMNeT++.

Los módulos que contienen submódulos son llamados módulos compuestos, al contrario de los módulos simples que están en el nivel más bajo de la jerarquía de módulo. Los módulos simples contienen los algoritmos del modelo. El usuario implementa los módulos simples en C++, usando la librería de simulación de clases de OMNeT++.

A3.2.2 Tipos de módulo

Tanto los módulos simples como compuestos son instancias de tipos de módulo. Mientras se describe el modelo, el usuario define el tipo de módulo; las instancias de ese tipo de módulo sirven como componentes para tipos de módulo más complejos. Finalmente, el usuario crea el módulo sistema como una instancia de tipos de módulo previamente definidos, todos los módulos de la red son instanciados como submódulos y sub-submódulos del módulo sistema.

Cuando un tipo de modulo es usado como un bloque de construcción, no se distingue entre si es un módulo simple o compuesto. Esto permite al usuario dividir un módulo en módulos simples dentro de varios módulos simples incrustados dentro de un módulo compuesto, o viceversa, agregar la funcionalidad de un módulo compuesto a un único módulo simple, sin afectar a los usuarios existentes del tipo de módulo.

Los tipos de módulos pueden ser almacenados en ficheros, separadamente del lugar donde están siendo usados. Esto significa que el usuario puede agrupar los tipos de módulo existentes y crear librerías de componentes. Para más información consultar [11].

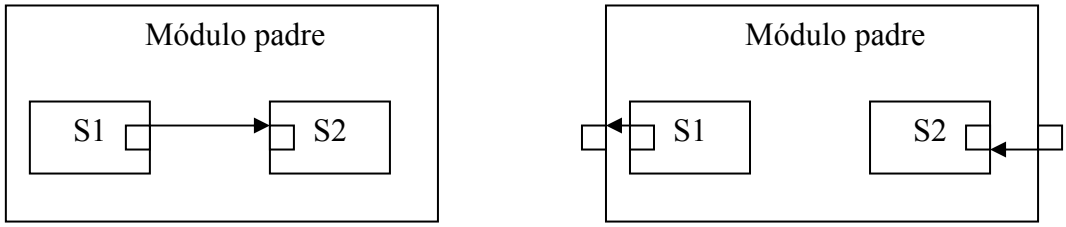
A3.2.3 Mensajes, puertas, conexiones

Los módulos se comunican mediante el intercambio de mensajes. En una simulación actual, los mensajes pueden representar tramas o paquetes en una red de ordenadores, procesos o clientes en una red de colas u otros tipos de entidades móviles. Los mensajes pueden contener estructuras de datos arbitrariamente complejas. Los módulos simples pueden enviar mensajes o bien directamente a su destino o bien a lo largo de un camino predefinido, a través de puertas y conexiones.

El tiempo de simulación local del módulo avanza cuando el módulo recibe un mensaje. El mensaje puede llegar de otro módulo o del mismo módulo (los mensajes enviados a sí mismo se usan para implementar temporizadores).

Las puertas son los interfaces de entrada y salida de los módulos; los mensajes son enviados a través de puertas de salida y llegan a través de puertas de entrada.

Cada conexión (también llamado enlace) es creado dentro de un solo nivel en la jerarquía de módulos; dentro de un módulo compuesto, uno puede conectar las puertas correspondientes de dos submódulos, o una puerta de un submódulo y una puerta de un módulo compuesto (Fig. A3.2).



Submódulos conectados entre ellos Submódulos conectados al módulo padre

Figura A3.2 –Conexiones

Debido a la estructura jerárquica del modelo, los mensajes típicamente viajan a través de una serie de conexiones, para empezar y llegar en módulos simples. Tales series de conexiones que van entre módulos simples son llamadas rutas. Los módulos compuestos actúan como "cajas negras" en el modelo, transmitiendo mensajes transparentemente entre su mundo interno y externo.

A3.2.4 Modelado de las transmisiones de paquetes

A las conexiones se les pueden asignar tres parámetros, los cuales facilitan el modelado de las redes de comunicaciones, pero pueden ser útiles en otros modelos también: retardo de propagación, VER (Bit Error Rate) y velocidad de transmisión de datos, siendo los tres opcionales. Se pueden especificar los parámetros del enlace individualmente para cada conexión, o definir tipos de enlace y usarlos en el modelo completo.

El retardo de propagación es la cantidad de tiempo que se retrasa la llegada del mensaje cuando éste viaja a través del canal.

El VER especifica la probabilidad de que un bit sea transmitido incorrectamente, y permite un modelado simple de canales ruidosos.

La velocidad de transmisión de datos es especificada en bits/segundo, y es utilizada para calcular el tiempo de transmisión de un paquete.

Cuando se usan las velocidades de transmisión, el envío de mensajes en el modelo corresponde con la transmisión del primer bit, y la llegada del mensaje se corresponde con la recepción del último bit. Este modelo no es siempre aplicable, por ejemplo protocolos como Token Ring y FDDI (Fiber Optics Data Distributed Interface) no esperan la llegada íntegra de la trama, sino que empiezan a repetir sus primeros bits tan pronto como llegan – en otras palabras, las tramas fluyen "a través" de las estaciones, siendo retrasadas sólo unos pocos bits. Si se quiere modelar ese tipo de redes, la característica de velocidad de transmisión de OMNeT++ no puede ser usada.

A3.2.5 Parámetros

Los módulos pueden tener parámetros. Los parámetros pueden ser asignados o bien en los ficheros NED o bien en el fichero de configuración *omnetpp.ini*.

Los parámetros pueden ser usados para personalizar el comportamiento de un módulo simple, y para parametrizar la topología del modelo.

Los parámetros pueden tomar valores de *Spring*, *numérica* o *bolean*, o pueden contener árboles de datos XML (extensible Marcus Language). Los valores numéricos incluyen expresiones usando otros parámetros y llamando a funciones C, variables aleatorias de diferentes distribuciones, y valores de entrada interactivos con el usuario.

Los parámetros de valor numérico pueden ser utilizados para construir una topología flexible. Dentro de un módulo compuesto, los parámetros pueden definir el número de submódulos, el número de puertas, y la forma en que las conexiones internas están hechas.

A3.2.6 Método de descripción de la topología

El usuario define la estructura del modelo en el lenguaje de descripciones NED (Netwok Description). Para obtener más información sobre el lenguaje NED, consultar la referencia [11].

A3.3 Programación de algoritmos

Los módulos simples del modelo contienen algoritmos como funciones C++. La total flexibilidad y potencia del lenguaje de programación puede ser usado, soportado por las librerías de simulación de clases de OMNeT++. El programador de la simulación puede escoger entre descripción “event-driven” o “process-style”, y puede usar libremente los conceptos de orientación a objetos (herencia, polimorfismo, etc.) y diseñar plantillas para extender la funcionalidad del simulador.

Los objetos de simulación (mensajes, módulos, colas, etc.) están representados por las clases C++. Han sido diseñados para trabajar conjuntamente de forma eficiente, creando una potente estructura de simulación programada. Las siguientes clases son parte de la librería de clases de simulación:

- módulos, puertas, conexiones, etc.
- parámetros
- mensajes
- contenedores de clases (p.ej. colas, arrays)
- clases de colección de clases
- clases de estimación y distribución estadística (histogramas, algoritmos para cálculo de percentiles, etc.)
- clases de detección de transitorios y de exactitud de resultados

Las clases están especialmente dotadas, permitiendo recorrer objetos de una simulación en proceso y mostrar información sobre ellos como el nombre, el nombre de la clase, el estado de las variables o los contenidos. Esta característica ha hecho posible crear un interfaz de usuario de simulación donde todos los objetos internos de la simulación son visibles.

A3.4 Usando OMNeT++

A3.4.1 Construyendo y ejecutando simulaciones

Esta sección permite entender mejor como trabajar con OMNeT++ en la práctica. Temas como modelos de fichero, compilación y ejecución de las simulaciones son tratados a continuación.

Un modelo OMNeT++ consta de las siguientes partes:

- Descripciones de las topologías en lenguaje NED (ficheros *.ned*) los cuales describen la estructura del módulo con parámetros, puertas, etc. Los ficheros NED pueden ser escritos usando cualquier editor de texto o el editor gráfico GNED.
- Definiciones de mensajes (ficheros *.msg*). Se pueden definir varios tipos de mensajes y añadir campos de datos a ellos. El programa OMNeT++ traducirá la definición de los mensajes a las clases C++.
- Las fuentes de módulos simples. Son ficheros C++, con sufijos *.h* y *.cc*.

El sistema de simulación proporciona los siguientes componentes:

- Kernel de simulación. Contiene el código que la simulación y la librería de clases de la simulación. Está escrito en C++, compilado y añadido conjuntamente para formar la librería (ficheros con extensión *.a* o *.lib*).
- Interfaz de usuario. Las interfaces de usuario de OMNeT++ son usadas en la ejecución de la simulación, para facilitar el *"debugging"*, pruebas, o ejecuciones de series de simulaciones. Hay varios interfaces de usuarios, escritos en C++, compilados y añadidos de forma conjunta en librerías (ficheros con extensión *.a* o *.lib*).

Los programas de simulación están construidos sobre varios componentes. Primero, los ficheros *.msg* son traducidos a código C++ usando el programa *"opp_msgc"*. Entonces todas las fuentes C++ son compiladas, y *"linkadas"* con el kernel de simulación y la librería de interfaz de usuario para formar el ejecutable de simulación. Los ficheros NED pueden o bien ser también traducidos a C++ (usando *"nedtool"*) o bien *"linkados"* dentro, o cargados dinámicamente en sus formas originales de texto cuando el programa de simulación empieza.

Ejecutando la simulación y analizando los resultados

El ejecutable de la simulación es un programa autónomo, el cual se puede hacer funcionar en otras máquinas sin OMNeT++ o sin que los ficheros modelo estén presentes. Cuando el programa es iniciado, lee el fichero de configuración (normalmente llamado *"omnetpp.ini"*). Este fichero contiene ajustes que controlan como será ejecutada la simulación, valores para los parámetros de los modelos, etc. El fichero de configuración puede también prescribir varias ejecuciones de simulación; en el caso más simple, será ejecutada por el programa de simulación una después de otra.

La información de salida de la simulación es escrita en ficheros de datos: ficheros vector de salida, ficheros escalares de salida, o los posibles ficheros de salida propios del usuario. OMNeT++ proporciona una interfaz de usuario llamada *"Plove"* para ver y dibujar los contenidos de los ficheros vector de salida. No se espera que alguien pueda procesar los ficheros resultado usando simplemente OMNeT++: los ficheros de salida son ficheros de texto en un formato que puede ser leído en paquetes de software matemático como Matlab o Octave, o importados a hojas de cálculo como OpenOffice Calc, Gnumeric o MS Excel (algún preprocesado usando *"sed"*, *"awk"* o *"perl"* puede ser requerido). Todos estos programas externos proporcionan una rica funcionalidad para análisis estadísticos y visualización.

Los ficheros escalares de salida pueden ser visualizados usando la herramienta *"Scalars"*. Éste puede dibujar diagramas de barras, dibujos en coordenadas x-y (p.ej Tasa de salida neta vs tasa de entrada), o exportar datos vía el portapapeles para obtener un análisis más extenso en una hoja de cálculo o en otros programas.

Interfaces de usuario

El primer propósito de las interfaces de usuario es hacer los parámetros internos del modelo visibles al usuario, para controlar la ejecución de la simulación, y posiblemente permitir al usuario intervenir cambiando variables/objetos dentro del modelo. Tan importante como lo anterior es permitir de forma práctica al usuario experimentar el comportamiento del modelo. El interfaz gráfico de usuario puede también ser usado para demostrar el modo de operar del modelo.

El mismo modelo de simulación puede ser ejecutado con diferentes interfaces de usuario, sin ningún cambio en los ficheros modelo. El usuario testearía y depuraría la simulación con un potente interfaz gráfico de usuario, y finalmente la ejecutaría con un simple y rápido interfaz que soportaría la ejecución por lotes.

Librería de componentes

Los tipos de módulo pueden ser almacenados en ficheros separados del directorio de uso. Esto permite al usuario agrupar tipos de módulos existentes y crear librerías de componentes.

Programas autónomos de simulación

Un ejecutable de simulación puede almacenar varios modelos independientes que usan la misma serie de módulos simples. El usuario puede especificar en el fichero de

configuración qué modelo va a ser ejecutado. Esto permite un extenso ejecutable que contenga varios modelos de simulación, y distribuirlo como una herramienta de simulación autónoma. La flexibilidad del lenguaje de descripción topológica también soporta este modo de operar.

A3.4.2 Qué hay en la distribución

Si se ha instalado la distribución de OMNeT++ sin personalizar, el directorio "omnetpp" en el sistema debería contener los siguientes directorios. (Si se ha instalado una distribución precompilada, algunos de los directorios pueden faltar, o quizás hay directorios adicionales).

La estructura de directorios del sistema de simulación es la siguiente:

omnetpp/	Directorio raíz de OMNeT++
bin/	Ejecutables de OMNeT++ (GNED, nedtool, etc.)
include/	Ficheros de cabecera de los modelos de simulación
lib/	Ficheros de librería
bitmaps/	Iconos que pueden ser usados en los gráficos de red
doc/	Manual (PDF), léeme, licencia, etc.
manual/	Manual en HTML
tictoc-tutorial/	Introducción al uso de OMNeT++
api/	Referencias API (Application Program Interface) en HTML
nedxml-api/	Referencias API para la librería NEDXML
src/	Fuentes de la documentación
src/	Fuentes OMNeT++
nedc/	Nedtool, compilador de mensajes
sim/	Kernel de simulación
parsim/	Ficheros para la ejecución distribuida
netbuilder/	Ficheros para leer dinámicamente los ficheros NED
envir/	Código común para los interfaces de usuario
cmdenv/	Línea de comandos de la interfaz de usuario
tkenv/	Interfaz de usuario basado en Tcl/Tk
gned/	Editor NED gráfico
plove/	Analizador del vector de salida de info y herramienta de dibujo
scalars/	Analizador de la salida escalar de info y herramienta de dibujo
nedxml/	Librería NEDXML
utils/	Creador makefile, herramienta de documentación, etc.
test/	Suite de test de regresión
core/	Suite de test de regresión para la librería de simulación
distrib/	Suite de test de regresión para distribuciones *"built-in"*
…	

Las muestras de simulaciones están en el directorio *"samples"*.

samples/	Directorios para las muestras de simulaciones
aloha/	Modelos del protocolo Aloha
…	

Directorio *"contrib"* contiene material de la comunidad OMNeT++.

contrib/	Directorio para el material aportado
octave/	Scripts Octave para el procesado de resultados
emacs/	Sintaxis NED destacada para Emacs

También se pueden encontrar directorios adicionales como *mscv/* , los cuales contienen componentes de integración para Microsoft Visual C++, etc.

A3.5 Modelos y parámetros

Para poder realizar la simulación de la arquitectura diseñada se han creado 11 modelos diferentes, las funciones de la gran mayoría se han explicado anteriormente. Estos 11 modelos son los siguientes:

AA → Simula el comportamiento del Servidor de Autenticación y Autorización.

Colas → Simulan la función de buffer de las otras entidades, para que no se pierdan paquetes y se puedan almacenar de forma momentánea hasta poder ser servidos. Cada entidad tiene su propia cola. En el caso del ES, se dispone de una cola para las peticiones de traspaso y otra para las peticiones de nuevo servicio, dándole más prioridad a la de traspasos.

CT → Simula el comportamiento del Contenedor de Información de la red actual de conexión.

CT_o → Simula el comportamiento del Contendor de Información de la red anterior a la que estaba conectado el terminal móvil.

ES → Simula el comportamiento del Elemento de Servicio que recibe las peticiones de creadas por los terminales de usuario.

FGT → Simula el comportamiento de la Función de Gestión de la Tarificación de la red actual de conexión. (Es la que contiene la parte de código más compleja).

FGT_n → Simula el comportamiento de la Función de Gestión de la Tarificación propia de cada subred a la que el usuario puede ser conectado. (Tiene un comportamiento mucho más simple que la anterior).

FGT_o → Simula el comportamiento de la Función de Gestión de la Tarificación propia de la red anterior a la que estaba conectado el terminal móvil. (Se suele utilizar básicamente como entidad de paso para consultas sobre información de traspasos y de autenticación).

Resultado → Se utiliza básicamente para obtener informes de los retardos que experimentan los mensajes desde que se crea la petición hasta que el terminal móvil es conocedor de qué se está sirviendo. Aporta información estadística como el retardo promedio, el retardo máximo y la desviación estándar del retardo al servir peticiones tanto de nuevo servicio como de traspaso.

SM → Simula el comportamiento conjunto de la Sonda de Medición y el Elemento de Servicio. Gestiona el nivel de recursos restante de la red y va enviando al CT correspondiente la información actualizada del nivel de ocupación de sus recursos.

TU → Simula un conjunto de usuarios móviles, generando peticiones de traspaso y de nuevo servicio según la probabilidad ajustada para cada uno y según la tasa de generación global deseada. Además en cada petición generada se establece el tipo de servicio.

Cada modelo programado en C++ tiene determinados parámetros ajustables, los cuales están especificados en el fichero *"omnetpp.ini"*. En la mayoría de los modelos hay un parámetro de tiempo de procesado, el cuál hace referencia al tiempo que tarda la entidad en procesar un mensaje recibido y actuar en consecuencia. Además de este parámetro común en la mayoría de las entidades, hay otros parámetros específicos de cada entidad, como por ejemplo los siguientes:

TU → *Distribución de la población de servicio:* Establece el porcentaje de servicios que estarán destinados a datos y a voz.

Tasa de traspasos y nuevos servicios: Especifica que cantidad de las peticiones están destinadas a traspasos y a nuevos servicios.

Tamaño de las ráfagas: Especifica que cantidad de peticiones llegan en un mismo intervalo de tiempo.

Tiempo entre cada petición dentro de la ráfaga: Especifica que intervalo de tiempo hay entre las peticiones que se generan dentro de una misma ráfaga. Este tiempo es una variable aleatoria exponencial.

Tiempo entre ráfagas: Establece la separación temporal entre una ráfaga y la siguiente. Este tiempo también es una variable aleatoria exponencial.

SM → *Capacidad:* Especifica la cantidad de recursos de que dispone para servir las peticiones. Este valor dependerá del tipo de red, para UMTS por ejemplo será mayor que para GSM.

Retardo: Especifica el retardo que introduce la red en el tratamiento de las peticiones recibidas. A mayor carga se irá incrementando el valor de este retardo.

Recursos ocupados para datos y voz: Especifica la cantidad de recursos necesarios para servir un servicio de voz y de datos respectivamente. La cantidad de recurso necesario se le restará a la capacidad total de la red mientras se esté proporcionando el servicio.

Duración de los servicios: Especificará el tiempo estimado de duración de un servicio de voz o bien de datos. Este valor es una variable uniforme.

Tipo de red: Especificará el tipo de red de que se trata (UMTS, GSM, …).

FGT → *Tipo de autenticación:* Establece si en la simulación se va a realizar una autenticación en serie o en paralelo.

Tipo de escenario: Establece si el usuario está inicialmente conectado a su Home Operator o no.

Colas → *Capacidad:* Establece el tamaño que tendrá la cola. No todas las entidades tienen la misma capacidad. Ésta dependerá del volumen de mensajes procesados que tenga la entidad, por ejemplo, la entidad con mayor tamaño de cola es la FGT.

Finalmente, aparte de todos estos parámetros correspondientes a determinados modelos también hay parámetros que afectan a la simulación global aunque en nuestro caso sólo hemos utilizado uno, el tiempo de simulación, el cual ha sido de 5 horas (18000 s).

A continuación, a modo de ejemplo se añade el fichero *"omnetpp.ini"* utilizado en alguna de las simulaciones, para tener una idea palpable de los conceptos expuestos anteriormente.

```
[General]
preload-ned-files=*.ned
sim-time-limit = 18000s
network = escenariob

[Parameters]
escenariob.numRedes=4

#Configuración de las colas de los sistemas
#*****************************************************************
*.Cola_FGTo.tipo_cola=0
*.Cola_FGTo.capacidad = 74
*.Cola_FGT1.tipo_cola=1
*.Cola_FGT1.capacidad = 74
*.Cola_FGT2.tipo_cola=2
*.Cola_FGT2.capacidad = 80
*.Cola_FGT3.tipo_cola=3
*.Cola_FGT3.capacidad = 80
*.Cola_CT.tipo_cola=4
*.Cola_CT.capacidad = 74
*.Cola_AA.tipo_cola=5
```

```
*.Cola_AA.capacidad = 74
*.Cola_CTo.tipo_cola=6
*.Cola_CTo.capacidad = 74
*.Cola_AAo.tipo_cola=7
*.Cola_AAo.capacidad = 74
*.Cola_ESc.tipo_cola=8
*.Cola_ESc.capacidad = 10
*.Cola_ES.tipo_cola=9
*.Cola_ES.capacidad = 10
*.Cola_TU.tipo_cola=10
*.Cola_TU.capacidad=10
*.Cola_NS.tipo_cola=11
*.Cola_NS.capacidad = 40
*.Cola_HO.tipo_cola=12
*.Cola_HO.capacidad = 100
*.Cola_FGT.tipo_cola=13
*.Cola_FGT.capacidad = 500
*.Cola_ES1.tipo_cola=14
*.Cola_ES1.capacidad = 10
*.Cola_ES2.tipo_cola=15
*.Cola_ES2.capacidad = 10
*.Cola_ES3.tipo_cola=16
*.Cola_ES3.capacidad = 10

#Parametros del Terminal de usuario
#*****************************************************************
*.TU.tipo_peticion = bernoulli(0.40)
*.TU.frecuencia = 10
*.TU.tipo_servicio =  bernoulli(0.62)
*.TU.entre_rafagas =  exponential(5.0)
*.TU.entre_paquetes =  exponential(0.1)
#*****************************************************************

#Retardos de las diferentes entidades
#*****************************************************************
*.ES.retardo = uniform(0.4us,1.2ms)
*.FGTo.retardo = uniform(2us,10us)
*.FGT.retardo = uniform(2us,10us)
*.FGT.retardo_traspaso = uniform(60ms,64ms)
*.FGT.tipo_AA=1
*.FGT.escenario=0
*.FGT1.retardo = uniform(2us,10us)
*.FGT1.tipo_FGT=1
*.FGT2.retardo = uniform(2us,10us)
*.FGT2.tipo_FGT=2
*.FGT3.retardo = uniform(2us,10us)
*.FGT3.tipo_FGT=3
*.CT.retardo = uniform(3.06ms,3.5ms)
*.CT.costoumts = 1
*.CT.costogsm = 0.9
*.CT.numRedes = 4
*.CTo.retardo = uniform(3.06ms,3.5ms)
*.AAo.retardo=uniform(0.4us,1.2ms)
*.AA.retardo=uniform(0.4us,1.2ms)

#Parametros de configuracion de capacidad de redes
#*****************************************************************
*.ES1.capacidad=4500
*.ES1.retardo=30
*.ES1.datos=150
```

```
*.ES1.voz=36
*.ES1.t_datos=uniform(6s,8s)
*.ES1.t_voz=uniform(120s,150s)
*.ES1.tipo=0
*.ES1.ES=1

*.ESc.capacidad=12000
*.ESc.retardo=20
*.ESc.datos=150
*.ESc.voz=80
*.ESc.t_datos=uniform(6s,8s)
*.ESc.t_voz=uniform(120s,150s)
*.ESc.tipo=1
*.ESc.ES=0

*.ES2.capacidad=12000
*.ES2.retardo=21
*.ES2.datos=150
*.ES2.voz=80
*.ES2.t_datos=uniform(6s,8s)
*.ES2.t_voz=uniform(120s,150s)
*.ES2.tipo=1
*.ES2.ES=2

*.ES3.capacidad=4500
*.ES3.retardo=30
*.ES3.datos=150
*.ES3.voz=36
*.ES3.t_datos=uniform(6s,8s)
*.ES3.t_voz=uniform(120s,150s)
*.ES3.tipo=0
*.ES3.ES=3
```

A3.6 Ejemplos programación y escenarios

Finalmente, para tener una idea de algún caso práctico realizado se añade el código C++ del módulo que se ha programado para implementar el terminal de usuario:

```
#include <string.h>
#include <omnetpp.h>

class TU : public cSimpleModule
{
        private:
                double BL;                              // Especifica la frecuencia de las rafagas
                double BC;                              // Especifica la frecuencia de las peticiones dentro de las
rafagas
                double EB;                              // Especifica la frecuencia entre rafagas
                double EP;                              // Especifica la frecuencia entre paquetes dentro de la
rafaga
                int Tipo_Pet;                   // Especifica que tipo de peticion es 0 --> HO , 1 --> NS
                int Total_Pet;                  // Especifica el numero de peticiones totales
                int Total_HO;                   // Especifica el numero total de peticiones de HO
                int Total_NS;                   // Especifica el numero total de peticiones de NS
                int Tipo_servicio;    // Especifica el tipo de servicio que solicita la peticion 0 --> Voz , 1 --> Datos

        protected:
                virtual void initialize();
                virtual void handleMessage( cMessage *msg);
                virtual void TU::finish();
};

Define_Module(TU);
```

```
void TU::initialize()
{
	BL=(double) par("frecuencia");
	BC= BL;
	EB= (double) par("entre_rafagas");
	EP= (double) par("entre_paquetes");
	Total_Pet = Total_HO = Total_NS = 0;
	cMessage *msg = new cMessage("mensaje-inicial");
	WATCH(BC);
	scheduleAt(50,msg);
}

void TU::handleMessage(cMessage *msg)
{
	cMessage *msgParaEnviar,*gestion_externa;;
	char msgNombre[20];

	Tipo_Pet = (int) par("tipo_peticion");
	Tipo_servicio = (int) par("tipo_servicio");



	if (msg->isSelfMessage())
	{

		if (Tipo_Pet == 0)    // Si la peticion es un Handover (HO) ...
		{
			++Total_HO;
			++Total_Pet;
			sprintf(msgNombre,"HO_REQUEST_%d",Total_HO);
			msgParaEnviar = new cMessage(msgNombre,1); // HO --> kind = 1
			msgParaEnviar->setLength(Tipo_servicio);          // 0 --> Voz ; 1 --> Datos
			ev << "El tipo de servicio de la peticion es" << Tipo_servicio << ".\n";
			msgParaEnviar->setPriority(Total_HO); // Almacenamos el numero de peticion de HO que
es
			msgParaEnviar->setTimestamp();
			send(msgParaEnviar,"out",0);// Enviamos el mensaje a la Cola de Handovers (HO)
		}
		else        // Si la peticion es un Nuevo Servicio (NS) ...
		{
			++Total_NS;
			++Total_Pet;
			sprintf(msgNombre,"NS_REQUEST_%d",Total_NS);
			msgParaEnviar = new cMessage(msgNombre,0); // NS --> kind = 0
			msgParaEnviar->setLength(Tipo_servicio);          // 0 --> Voz ; 1 --> Datos
			ev << "El tipo de servicio de la peticion es" << Tipo_servicio << ".\n";
			msgParaEnviar->setPriority(Total_NS); // Almacenamos el numero de peticion de NS que
es
			msgParaEnviar->setTimestamp();
			send(msgParaEnviar,"out",1);// Enviamos el mensaje a la Cola de Nuevos Servicios (NS)
		}
		if (--BC==0) // Manipulamos los parametros de la rafaga de mensajes
		{
		  BC=(double) par("frecuencia");;
		  scheduleAt(simTime() + EB, msg);     // Programamos la ejecucion de la siguiente rafaga
		}
		else
			scheduleAt(simTime() + EP, msg);
	}
	else
	{
		if(msg->kind()==15)
			delete msg;
		else
		{
			send(msg,"out",2);  // Cuando recibamos la respuesta, la enviamos a la entidad
					    "Resultado"
			gestion_externa = new cMessage("IDLE_SERVER",15);     //Informamos a la Cola_TU
										de que el servidor esta
										parado
			send(gestion_externa,"out",3);
		}
	}

}
```

```
void TU::finish()
{
        ev << "Solicitudes totales generadas: " << Total_Pet << endl;
        ev << "Solicitudes de tipo traspaso: " << Total_HO << endl;
         ev << "Solicitudes de tipo nuevo servicio    " << Total_NS << endl;
        recordScalar("#Solicitudes totales",Total_Pet);
        recordScalar("#Solicitudes HO", Total_HO);
        recordScalar("#Solicitudes NS", Total_NS);
}
```

Como se puede observar, hay tres funciones básicas: inicialización, tratamiento de mensajes y final del procedimiento, las cuales se ejecutan de forma secuencial. A nivel general y sin entrar en detalle, la función de este módulo consiste en generar un tráfico a ráfagas de mensajes, bien de traspaso o de nuevo servicio según la frecuencia y la probabilidad especificada. Además, se calculan los retardos totales medios desde que se crea una nueva petición hasta que se sirve, y finalmente se muestran los datos por pantalla.

Finalmente, como ejemplo final, se muestra el escenario de simulación utilizado para evaluar el rendimiento de la arquitectura diseñada mediante la interfaz gráfica que ofrece OMNeT++:

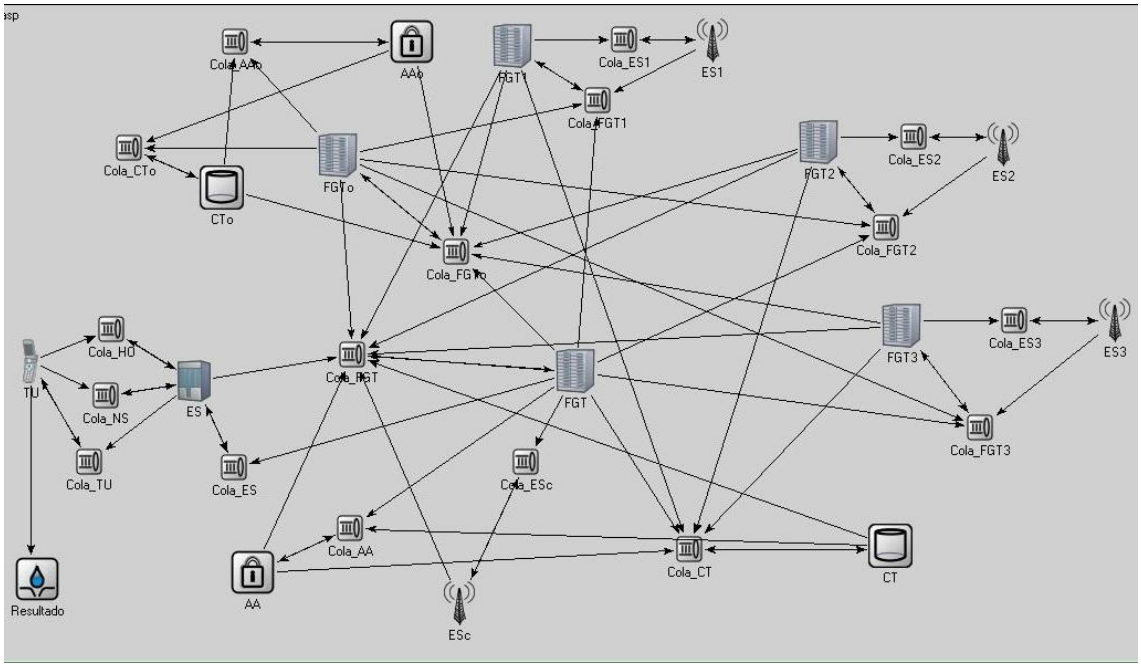


Figura A3.1 – Escenario de simulación

En el escenario de simulación de la imagen superior se pueden apreciar las diferentes entidades utilizadas, las cuales son las ya descritas previamente en este documento (FGT, CT, AA, ES,…). En cada entidad insertada, e incluso en las conexiones entre ellas se definen los parámetros de configuración que caracterizan su modo de operar, tal y como se ha comentado anteriormente.